前　言

2008年6月28日，中国财政部等五家政府部委联名下发了《五部委关于内部控制的通知》（财会[2008]7号）以及《企业内部控制基本规范》，明确规定作为一项义务，上市公司自2009年7月1日开始，需要对本公司内部控制有效性进行评价，同时披露年度内部控制评价报告。

作为世界经济大国之一的中国，继美国、日本之后，把导入严谨的内部控制自我评价报告制度的决定，作为经济上的一种基础设施来抓，可以说是有划时代意义的。

内部控制是什么？简而言之，就是“公司的管理是否妥当”。一般而言，“管理”这个词，可能会让人联想到票据的记账、审批的流程，会让人觉得费时低效。但是，请试想一下完全不存在管理的业务，如果经费的申请没有审批，经费就可能会使用过度；如果不经过新客户调查就把商品卖给他们，很有可能会造成应收账款不能收回。作为取得平衡的这种“管理”或者“内部控制”，对业务效率的贡献是毋庸置疑的。

因此，简单总结一下内部控制报告制度的要求，即“对外证明你们的公司，你们的部门，你自己恰当执行日常管理”。

那么，只要对自己公司业务有信心，觉得能顺利开展（尽管问题或者课题还是不少的，但显然大多数公司都认为自己业务顺利开展了），就可以安心吗？答案是否定的！因为在导入内部控制的过程中，还有不少地方必须要变革。

第一，要向第三方客观地显示“已经有良好的管理”是很不容易的。例如，尽管管理者认为“自己可以掌控部下实施的业务”，但对于没有书面证据的部分，作为第三方来说是无法判断的。

第二，“内部控制”的概念来自欧美，其内容中也包括了许多实务，且

这些实务到目前为止是中国或日本企业中还没有实施的新内容。

本书的目的，就是对复杂的“内部控制”进行简单易懂的说明。本书从实际的内部控制相关的咨询和审计的经验出发，介绍了概念源自欧美的内部控制在中国或者日本企业中运用时的各种小插曲，同时，也说明了中国、欧美、日本业务的相同以及相异点。

笔者希望这本书可以让各职能的企业管理人员广泛阅读。这些管理人员包括从构筑内部控制立场出发的财务部门、内控部门或者经营管理部门等，从评价立场出发的内部审计部门等，以及从业务出发的管理层人员等。

本书是在日本出版的《由内部控制而改变的现场工作》(Diamond 出版社，2007 年 3 月)的基础上，在原著者(原国太郎)赴任上海后，得到了德勤华永会计师事务所有限公司的合伙人丘仲文先生的大力支持，并与谈亮先生、钱莘女士一起对内容研讨，进行了大幅度的追加和修改而成。在此过程中，蒋薇女士、忻豪博先生、庄宇杰先生、姚承懿先生、秦杰先生、李莹女士、曹吉先生等也花费了大量的努力。在此，我们想对这些在辛勤工作之余，用自己的业余时间来帮助本书的编译工作的同事们表示最为诚挚的谢意！

另外，最后的第十八章、第十九章中，在说明内部控制评估制度组织的一般方法论的同时，对中国的《五部委关于内部控制的通知》、《企业内部控制基本规范》，以及财政部办公厅同时发布的《企业内部控制应用指引》、《企业内部控制评价指引》、《企业内部控制鉴证指引》等三个指导文件的征求意见稿进行了简单的说明。

本书的内容是以实务为基础的笔者的浅见，并不代表德勤华永会计师事务所有限公司的意见。另外，请了解，本书并没有完全罗列内部控制自我评价和内部控制审计过程中所有的相关控制点和检查点。

2008 年 9 月 10 日子夜

目　录

第一章 内部控制的基本概念

源自欧美的“应有的管理”

提起内部控制的概念和定义，美国的 COSO 内部控制整体框架[1]闻名于世。在日本版 SOX 标准的第一部分‘内部控制的基本框架’中，以及中国财政部等五部委在 2008 年 6 月 28 日发布的《企业内部控制基本规范》中也定义了内部控制。但是，在此我们先不谈那些生硬的内部控制的定义。此前，虽然内部控制没有得到正式的定义，但其概念早已形成。下面先介绍几个重要的内部控制的前提性基本概念。

预防性控制和检查性控制：事前还是事后

盖过章了吗？

员工：“谈部长又不在啊，小李，能帮我盖个章送到总务去吗？”

小李（事务员）：“好的。”

——几天后——

丘总：“谈部长！这张单据是你批准的吗？（怒）”

谈部长：“啊，实在对不起（汗）……（我盖过这个章吗？）”

说到‘内部控制’，一般立刻会联想到盖章或者签字，因为这象征了管理的手段。这个例子中，似乎没有部长的盖章批准，工作就无法向下开

展，这样的情况就是所谓的“预防性控制”。

与此对应，事后部长的上司发现了这张单据的错误。或许部长的上司只是偶然发现这张有问题的单据，我们假定这里是每月末对所有单据都检查一次，那么这就是所谓的“检查性控制”。

预防性、检查性等说法似乎是挺高深的，简而言之就是事前还是事后。另外还有补偿性控制、按风险是否可以接受设定的内部控制等的分类，这些都无需深究。

根据笔者的经验，在规章制度中定义这些行为有时也是项辛苦的咨询业务。

什么是“复核”？

审计人员：“让我们把事前控制称为批准。”

业务员：“就是说事后批准是不可以的了？”

审计人员：“事后控制称为复核怎么样？”

业务员：“看清单或者汇总表的倒还好，一件一件检查，似乎和‘复核’的含义不符啊。”

审计人员：“……”

因为这家公司用“审阅”这个词来折中表示“批准”和“确认”的意思，越说越复杂了。该公司最后将“批准”定义为“拥有事情决定权的管理者留下印迹表明其对内容的许可”；“审阅”定义为“没有事情决定权的管理者或担当人员留下印迹表明其对内容的认可”；“确认”定义为“不留印迹对内容进行检查”。上述全部为事前控制，事后的工作就全部定义为复核了。然后，以下我们对诸如已入账应付账款的讨论就可以表达为“账面记录的复核”、“支付前的审阅”等等。

批准、决议、审核、确认、检查、复核……到处都是术语。在制定、修订内部控制相关的制度、操作规程等的过程中，谁都会因此大伤脑筋的。

内部控制设计和运行状况：公司管理的体系以及制度的运行

内部控制的设计是指公司管理是怎样的体系、有什么制度。在第一个例子中，“部长检查了单据的内容，以盖章来表示他的批准”这样的制度，就是内部控制的设计。这是否是个适当的内部控制，仅看这一个例子是无法辨别的；我们注意到在上例中部长不在时，没有规定谁来执行代理其批准的权限，这虽然是件小事，但也可能是内部控制设计上的问题。

在这个例子中，实际是事务员代替盖的章，“没有按照制度运行”，这就是所谓的内部控制运行上的问题[2]。

职责分工：业务的全部流程不能都交给一个人负责

职责分工，即权限分离，是内部控制最重要的概念之一。其概念就是“一个部门、一个人不能掌管一个业务从头至尾所有的工作”。

最基本的职责分工是指一个业务的“业务记录、业务批准、实物管理”三个部分至少应该由不同的人（可能的话是不同部门）分别负责。尽管这样，实际业务流程中的分工往往更加细。公司应该结合成本效益原则和风险可控原则综合考虑。

以销售业务流程中理想的职责分工为例，其可分工为：

（1）订单记录；

（2）销售条款的批准；

（3）存货的保存管理；

（4）存货记录的保存；

（5）订单货物的出库；

（6）向销售方提出付款请求；

（7）应收账款记录的保存及批准；

（8）收款的处理；

（9）应收账款债权的跟踪；

（10）应收账款余额的确认及其对账差异的跟踪；

（11）客户管理主文档的变更；

（12）售后服务、反馈电话、投诉处理。

这么多！并非全部都要按其进行职责分工不可，但是根据不同的组合方式有以下三种情况："没有问题的组合"、"不太合适的组合"和"相当不合适的组合"。当然，根据实际情况，问题的性质也可能大相径庭。

此外，业务分工又可以分为横向分工和纵向分工这两种情况。

横向分工就是由几个部门或者业务分管人员共同参与到整个业务流程中。纵向分工就是业务分管人员负责制作和录入资料，业务主管负责批准以及复核资料，实际指的就是职责的分离。这种纵向分工，一方面要求管理人员来监督分管业务人员的工作，另一方面要求管理人员不能执行业务人员的工作。纵向分工的概念也令人感觉到内部控制这个概念的确是从欧美发展而来的。

这份单据我不能填！

谈部长："小庄，你来负责一下，根据这些条件来填一份单据吧。"

小庄："啊！部长，这个不太好吧（汗），我不能填（哭）。"

上述情况是内部控制所期望的事情。

大家一定会想："部长自己填个单据不就搞定了嘛！"，但是批准人自己填单据自己批准的话，无论怎么看都不太合适，属于利益冲突。

▼"内部控制"源自美国的全球化

毋庸赘言，当前的经营环境正在不断变化。就上述事例而言，如果假定代部长盖章的事务人员是"经关系单位介绍而被录用，就算辞职也是由

于和公司员工结婚而快乐离职”的人员，或者是“几个月前刚刚被人力资源服务公司派到公司来的派遣员工”，这两种情况是截然不同的。

不单是招聘方式的改变，经营指标、信息科技和金融工具等的改变，也使原本建立在社会基础上的公司的体系进入了调整的时期。从这个意义上说，无论是所谓“控制环境”的公司治理方向以及企业文化等重大课题，还是业务流程的内部控制，都将顺应世界潮流的发展。

这个变化正是源自美国的全球化进程的结果。同时对公司管理系统的审视也是以“内部控制”之名从美国舶来的。所以除了要建立在“人性本恶论”上去考虑内部控制，还需想象公司是在美国的环境中经营的。这样想的话，多少可以认同由此制度产生的文化差异。

内部控制的评价范围：影响财务报告的业务流程即为评价项目

一般情况下，内部控制的评价范围为图 1-1 中所列示的各部分[3]。但是类似在金融企业以及建筑施工企业等特殊行业中，由于使用的会计科目不同于其他行业，所以有必要针对这些特殊的业务追加实施内控评价。

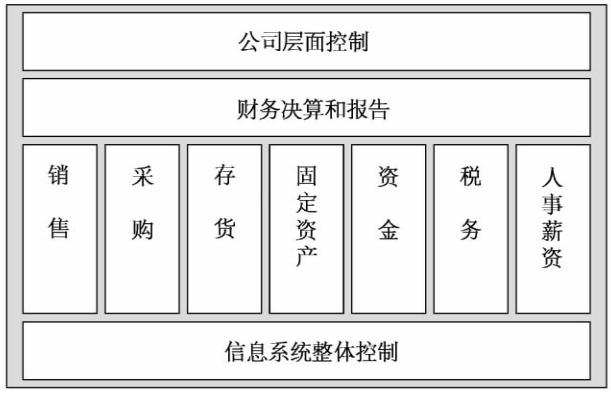

图 1-1　内部控制评价范围

在美国 SOX 法案中，与财务报表重要科目相关的业务流程全部会被纳入评价范围内，一般为图 1-1 中列示的所有业务流程。同时，2007 年 6 月公众公司会计监督委员会（PCAOB）颁布的《审计准则第 5 号》（AS5），强调了风险导向方法的重要性，企业自我评价以及外部审计的评价对象可以更侧重于承担高风险的项目。

在日本版 SOX 中，《实施标准》[4] 要求首先针对公司层面内部控制以及财务决算和报告流程两块内容进行评价，再决定去评价那些与企业经营目标密切相关的会计科目及其业务流程。举一个具有普遍性的例子来说（以一般经营业务的公司为例），《实施标准》重要的会计科目有“销售收入”、“应收账款”和“存货”，然后考虑与此相关的重要业务流程，各公司均基本会考虑针对“销售”、“存货管理”、“期末盘点”、“采购”以及“成本核算”流程来进行内控评价。因此，日本版 SOX 与美国 SOX 法案相比，企业的评价以及外部审计的测试项目数大幅减少。但是由于企业的实际主营业务不同，我们选择的所谓“与企业经营目标密切相关的会计科目及其业务流程”也有所不同。例如，在服务性行业中，公司可能需要评价其人事薪资流程。大型制造性企业有时也需要对其固定资产管理流程进行评价。此外，必须将高风险的业务个别追加纳入评价范围。《实施标准》具体举例，针对金融交易及衍生工具的交易、坏账准备及固定资产减值准备的计提、递延税款资产（负债）等方面进行评价。

中国财政部等五部委在 2008 年 6 月 28 日发布《企业内部控制基本规范》正式稿的时候，财政部办公厅同时发布了《企业内部控制应用指引》（征求意见稿），包含了 22 个具体的业务流程。从该应用指引来看，中国更多地借鉴美国 SOX 法案的做法，内控评价涵盖的业务流程要多于日本版 SOX。

- 资金
- 采购
- 存货
- 销售
- 工程项目
- 固定资产
- 无形资产
- 长期股权投资

- 筹资
- 预算
- 成本费用
- 担保
- 合同协议
- 业务外包
- 对子公司的控制
- 财务报告编制与披露
- 人力资源政策
- 信息系统一般控制
- 衍生工具
- 企业并购
- 关联交易
- 内部审计

内部控制的基本概念就先说到这里，接下去的各章会从各个不同领域探讨有关内部控制的具体情况。

[1] 1992 年美国的 COSO 委员会(the Committee of Sponsoring Organizations of the Treadway Commission)发表的报告，该文献从此成为世界性的内部控制的参照标准。

[2] 内部控制缺陷的定义和分类：根据中国财政部办公厅此次同时发布的《企业内部控制评价指引》(征求意见稿)，内部控制缺陷是指企业在内部控制中，出现以下几种情况之一：

1) 未实现对应控制目标；

2) 未执行规定控制活动；

3) 突破规定的权限；

4) 不能提供控制运行有效的相关证据。

在该指引中，内部控制缺陷按问题所在环节分为设计缺陷和运行缺陷：这很好理解，是与上文所述的内部控制的设计和运行状况相呼应的：在哪个环节发生的问题，就是哪个环节的缺陷。内部控制缺陷的第 1)种情况构成内部控制设计缺陷；第 2)到第 4)种情况构成内部控制运行缺陷。

另外，该指引将问题点定义为“重大缺陷”、“重要缺陷”和“一般

缺陷”三类。这种分类方法与美国相关监管机构对于内部控制按严重程度的分类保持了一致。当然，按严重程度分的三类与前述按问题所在环节分的两类并不矛盾，而是相互组合的关系。例如：某项“重大缺陷”既可能是“设计缺陷”，也有可能是“运行缺陷”。

[3] 这样的业务领域也在某些文献中被称作为“业务循环”。业务循环就是考量财务报告内部控制的评价单位，归集了相关会计科目以及报表披露项目，对应了一系列的业务流程。具体可参照第五章的“业务循环”一节。

[4] 关于日本版 SOX 的《实施标准》请参照第十八章（专栏）“日本版 SOX 相关规定的概要”。

第二章　销售(1)：接受订单、信用、价格

企业关注什么？

接受订单：接受订单时，无需制作会计分录，但在业务上和内部控制上都是相当重要的

折扣由业务员来决定？

销售经理："唉，我们的业务员都很忙，在系统中输入订单的工作常常会拖后。"

审计员："这样啊？"（笑眯眯）

销售经理："业务员有权决定一部分的折扣额度。"

审计员："是吗？"（吃惊）

销售经理："我们设定了付款信用额度，但基本上只是个形式，如果超额了也只是增加额度而已。"

审计员："这样啊……"（欲哭无泪）

对很多企业来说，销售是最受关注的工作。各企业为了生存和发展每日不停地互相竞争、短兵相接，争夺订单。

但是和接受订单在商务活动中所受到的高度重视相比，它在内部控制领域就显得比较薄弱。因为接受订单活动不需要制作会计分录，甚至有更极端的意见说——"接受订单根本是和财务内部控制完全无关的活

动”。但实际上，我们收到订单数据后，再按照“出货→实现销售→开发票发付款通知→收款”一环紧扣一环的顺序来开展业务，因此接受订单当然是不能忽视的重要内容。

建议公司针对订单内容有无正确录入进行确认。此外，向客户确认订单有无重复或者遗漏也很重要，尤其在下订单的频度较少、但订单的平均金额较大的行业。此外，比如建筑业和设备制造业，在接受订单以前的工程估算等工作，也可能是个更为重要的业务程序。

然而，在采购流程中，由于可能存在暗箱操作等潜在的舞弊风险，所以发出采购订单时，没有获得批准就去执行基本是不可想象的事情。与此相应，一般在接受销售订单时，业务员基本只要“在批准的价格和信用额度内”进行个人判断即可。

授信制度：信用管理现状以及企业文化

笔者所在的会计师事务所对内部控制进行评价时，拥有自己独有的内部控制评价数据库。根据数据库列示的内部控制要求，“对于超出授信额度的订单不予处理”如果现行内部控制系统中该控制不到位，就会被评价成“内部控制系统可能存在缺陷”。

在大多数集成化管理信息系统中，能够设定授信额度，并在超出授信额度时自动进行预警或者提示错误信息。

在日本，授信额度往往会成为业务流程内部控制评价中最易成为瓶颈的一个项目。实际上，大多数欧美企业，以及日本企业的海外子公司都会设定信用额度，超过额度时系统就会停止出货。与此相对，日本本土企业要么没有设定授信额度，要么就是马虎地设了个很大的授信额度，或者授信额度超额照样出货。上述情况非常之多。为何日本企业在日本本土对于信用额度的设定如此不重视呢？

日本企业曾经最重视的业绩指标就是营业额。这也可能是因为日本

企业长期以间接融资的手段进行资金筹措,另外关联企业互相持股,公司并不重视股东利益。日本企业中对于员工采取长期雇佣、论资排辈的制度,社会的贫富差距也不大。这种经营习惯和业绩评价指标,曾经一度有效地发挥了作用,带动了社会的发展。但是,这种环境随着泡沫经济的破灭,一切都或多或少地发生了变化。

日本企业这种轻视利润的倾向与其忽视授信额的做法,两者之间有着密不可分的关系。近年来,有些公司开始专注利润,以各事业部或者部门为单位开始进行业绩考核。但是基层人员在日常工作以及个人意识中,仍然很少体现出其重视利润的观念。

然而对于重视销售的公司来说,为了扩大销售,只要公司最终有利润能维持经营,并不在乎承担较大的授信风险。反正先确认销售,最终不过是会计处理时提个坏账而已。因此,对于这样的公司来说,严格推行授信制度的观念恐怕难以深入人心。

然而在美国,判断企业业绩最重要的指标是公司的利润。因此,形成了与其对应的社会形态结构和商业习惯。股票市场(→股东→利润)作为其社会性的基础设施,地位极其重要,然而相继发生的安然事件、世通案件等粉饰报表的经济丑闻案后,造成公众对披露信息的不信任,对社会产生了严重影响。

在中国,信用销售(赊销)的现象根据行业不同,也大量存在。但是,把它作为内部控制中的重要环节来认真对待,也就是最近这两年才发生的事情。

中国的销售模式与欧美和日本相比,款到发货的销售模式仍占较大比重。原因之一是在传统的商业习惯中,经常延迟付款,企业的观点就是"没有付款时,公司就占有主动"。(在日本,对于延迟付款的处罚是非常严格的,如果企业六个月以内两次不准时承兑票据,将被停止与银行交易,这样实际上也就意味着公司倒闭。)但是在中国没有这种商业习惯,这也就限制了中国企业间相互授予信用额,从而影响了销售规模。

给予客户适当的信用额度,这一点可对公司的业务发展起到很大的

推波助澜的作用。例如公司的销售主要是通过代理商为主时，如果不给予代理商一定的信用额度，代理商根据手头现金流状况，只能选择与付现款的最终客户进行交易，这样大大限制了代理商的发展空间 如果能够给予代理商一定的信用额度，分销就可以不受现金流的限制，积极开拓其市场占有率，更能提高公司的销售额。

在当前中国的企业发展中，是否给予最终用户和代理商各自适当的信用额，并对其信用状况如何作出合理评估，是相当有必要考虑和探讨的一个问题。此外，如果客户发生延付货款的情况，还需要酌情考虑取消其信用额度或者降低其信用额度。

恰当估计客户是否存在付款延迟或者无力付款等风险，这个工作并不简单。也不能因为客户之前经营状况良好，就放弃“慎重评估”。这个事情马虎不得。而且一旦根据能够接受的风险程度设定了适当的授信额度，就应该严格遵守，这是维护公司的利益所不可欠缺的。

另外，对于授信额度的设定主要有两种方法：一是在接受订单时检查“未发货订单余额＋应收账款余额”；二是在发货时检查“应收账款余额”。前者的做法更为普遍。主要是因为公司一旦接受了订单，将会承担采购原材料以及进行生产的风险。另外一个原因可能是公司委托第三方物流公司负责物流环节，或者由供应商直接发货给客户。这些公司在出货时检验授信额度的难度较大，因而多采用第一种方式计算授信额度。

价格：内部控制上，只要价格得到“批准”就万事大吉了吗？

在接受销售订单的过程中，与授信制度相比，接受订单价格这一环节在内部控制上出问题的概率较小。这是因为，实务中，基本上所有的销售经理对销售价格都是一清二楚的。另有很多公司，根据其明文规定或者不成文的习惯，对所有销售订单上的条件都必须进行审批，销售价格的折扣过低都是需要进行事前审批的。在本章开篇的例子里，“业务员有权决

定一定额度内的折扣”,建议公司最好明文规定把“一定额度”的折扣在内容上进行明确。如果折扣超过一定比率,管理层进行事先批准的话,可以判断为内部控制运行有效。并且在这种申请单据或销售合同上,通常就会有“经理”、“部长”确认后在相应位置上签字或盖章,这也可以作为管理层对单据进行审批的证据。此外,内部控制评价时也需要留意这种审批是否只是形式化的表面文章,还要关注如何处理例外事项。

▼ 从经营理念上出发,还有很多地方应该考虑

但是,即使内部控制体系上没有问题,从重视利润的角度来分析,对销售价格也还有很多必须要考虑的地方。

当以营业额作为业务员的业绩考核标准时,10%的折扣率对其业绩的影响只有 10%;但是如果以毛利为指标的话,假设原定价毛利率为20%,那么 10%的折扣率会使其业绩下降 50%。

因此,在认真探讨公司的授信制度的同时,应该也要考虑公司现有机制是否能够适应企业经营目标。

在此我们并不是说无需关注营业额指标。针对销售部门,营业额仍然应当作为考核日常工作的重要指标,但是有时候也要根据企业实际经营结构来分析。当企业需要扩大销售规模,有时需要必须先盈利,再以获得的利润为基础,去扩大销售规模。例如,企业需要依托投资来扩大规模时,只有先有了足够的利润,才能进一步考虑扩大规模。

过去在日本,只要公司的营业额能够增长,就不愁从银行借不到钱。但在世事变迁的今天,这种行为被认为是公司不健康的成长。美国的“内部控制”也是上述顺应时代潮流发展的产物之一。

在中国,不同企业的管理成熟度不同,对于价格管理的重视和相关内部控制的设计、运行的情况也有较大的不同。处于创立初期的私营企业主由于是最高管理者,也就是企业老板的一言堂,价格多数是由该老板直接参与制定,相对来说不太会有太多的价格管理相关的内部控制。而对于具有一定规模的本地企业和国有企业来说,价格的制定工作受到传统计

划经济体制的影响较多，多数是有着一定的流程、依据一定的方法来确定的，并在销售工作中予以体现；但是当企业成长到一定规模之后，有可能存在同一个企业集团不同地区的销售为了自身业绩，对于同一个产品互相压价的价格管理混乱的情况。当然，也有价格管理非常完善的企业，有见过采用包括出具季度指导价、信息系统控制价格等各种好的做法的企业。

专栏　供应链和企业财务，泡沫和泡沫破裂

笔者过去曾专门从事供应链管理流程的咨询业务。狭义的供应链管理是通过提高生产制造、库存、销售的信息传递效率来减少库存，广义的供应链管理就需要考虑包含产品开发的市场企划以及针对经营模式进行再考量。

提到供应链管理，戴尔电脑的例子是最具典型性的。先从网上接收订单，再进行生产，实现零库存（根本无需考虑由于存货的周转慢产生残次冷背产品），从客户处收回货款的时点甚至早于支付原材料货款。从资金流角度分析，这正是各个企业都梦寐以求的商业模式。

• 供应链和财务数据

下面是某个半导体制造企业供应链管理项目的例子。

提起半导体，人们也可能想象这应该是最先进产业，产品生产都是全自动的行业。半导体制造业分为前端和后端。其后端是通常被称作为组装的程序，属于劳动密集型流程。前端的工序却是高度依赖于机器装备，设备精密而又昂贵。是不断追求更先进的加工设备还是在仅有的产能下合理对其进行分配，这是个很重要的经营课题。最终的产品种类繁多，但它们的原料都是来自于晶圆。前端工序进行了一半以后，大规模集成电路等产品根据订单生产，而内存条等产品的产量完全基于预测，从供应链角度看，这真是个非常有趣的行业。

这个项目就是根据多种产品的订单数量和销售预测数量，归集生成产成品及半成品的库存数量，通过利用各工序的生产计划信息，使整个制造

计划阶段实现信息一体化，以达到减少存货量、提高净资产收益率(ROE)财务指标数值的目的。

但是，随着项目的开展，能够明显感到产品品种繁多带来的越来越多的负面影响(已经超出了原本供应链管理项目的实施范围)。产品品种一多，库存自然就大。工厂为了保证产能满负荷运转，不得不生产一些规格通用的产品(这样的话，设备折旧率分摊到单个产品上的成本就会降低，从工厂的角度来说也是可以理解的事情)。另一方面，销售部门因为重视营业额而滥用折扣。如此往复，利润当然不可能得到有效增加了。

结合起来看，可以说上述很多问题都与重视营业额(轻视利润)的习惯做法和业务组织架构有关。对企业主打的产品来说，企业在重视考虑营业额的情况下(只要保证还处在盈亏临界点之上)，销售该商品有利润(前提是要卖得掉)，公司就应该尽可能地完全生产这种产品。但是在重视利润的前提下，需要突出发展最能出规模效益的商品(或商品系列)。举几个同类的国外公司的例子，比如英特尔专业生产 CPU、德州仪器(TI)公司专业生产数字信号处理产品(DSP)、韩国的三星半导体部门专业生产内存，这种有的放矢的生产相应带来的就是高回报。

•“公司是谁的”这个问题与日本泡沫经济以及当前中国经济发展

针对“企业是为什么存在的?”这个问题，美国大多数企业的回答是“为了股东利益”。但是，在日本认为是“除了为股东还有为员工、客户等相关各方持股人”的企业很多。正如半导体行业被称作“工业的粮食”一样，很多的产业都离不开它，像刚刚列举的这个企业，它们也肩负了满足社会需求的使命。

在欧洲，通常会认为企业是社会的“公共资源”。讲句题外话，会计记账体系有英美式、大陆式(起源于法国、德国)的分类，前者的传统是重视利润表，后者则更重视资产负债表。这好像也比较符合富于冒险精神领导世界潮流的盎格鲁—撒克逊民族和致力于社会安定的欧洲大陆的形象。

在中国，企业的形式多样，虽然不能一概而论，但除外资企业以外主要可以分为国有企业和私营企业。如果说国有企业是为了“国家和人民而存在的”，那么私营企业可以说是“老板个人”的吧。在实际运作中，越来越多的中国企业采用了美国式的观点，强调股东价值最大化。对于国有企业来说，其大股东是国资委，即“国有资产管理委员会”；对于上市公司，则毫无疑问是持有其股票的股东；对于私营企业来说，股东即是老板个人。

回到以前的日本，由于企业都是相互持股，企业就缺失了真正的股东的概念，所以公司的存在价值就是为了员工和客户。就能非常自然地理解企业的存在是为了“社会的利益”。这种价值观可以说是在日本社会贫富差距小、追求中庸的文化背景及社会环境下形成的。资金的来源不是有钱的个人而是来自银行或者企业，资金融资方式也多是以间接融资为主。雇佣制度也是出于从员工角度出发，采取终生雇佣制。论资排辈的管理方式也就很自然地和传统的日本式/模仿式的经营理念相吻合。

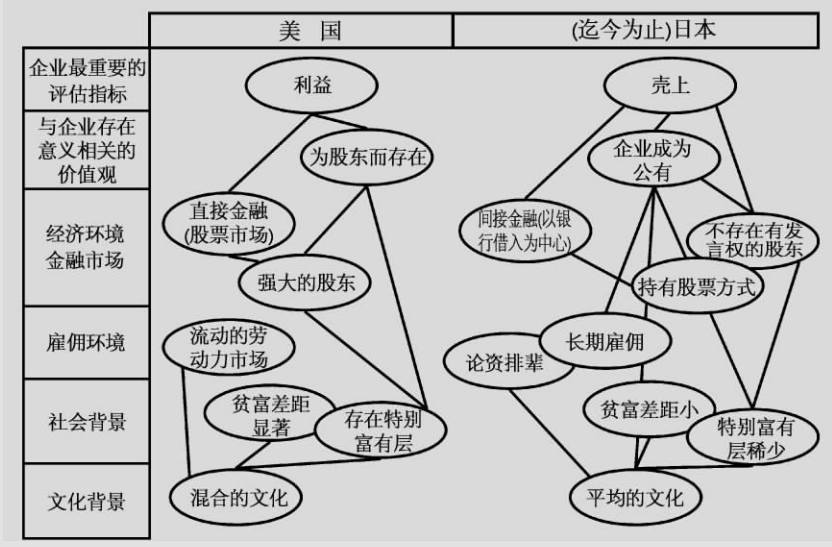

图 2-1 企业所处环境要素之间相互关联的示意图(美国、日本)

企业内外这些各种各样的要素有机地融合在一起，成为一个社会体系。在混沌(Chaos)理论中，曾经将社会作为一个“体系”进行研究，如果把“社会”称作体系，那么社会、文化环境就是“森林(植物)”，人是昆虫(?!)，企业是鸟或兽，整个系统内的各个角色相互依存、相互影响。

日本经济从1980年代后半叶到1990年代前半叶，遭遇了所谓的泡沫经济。经济发展前途一片看好，股价高涨，房价猛升，在这样一个资产大增的经济背景下，日本企业收购了美国的帝国大厦(Empire State Building)，成为了当时的热门话题。1990年1月日本股票市场开始暴跌，房产投资也开始走下坡路。从此，日本经济一蹶不振。

引起泡沫经济的主要原因是上述体系中各要素的互相作用：对利润的忽视、对不动产的现金流利润的无视、过度依赖间接融资随意获得资金、农耕民族式土地神话……从一定意义上讲，过度投机狂潮之后就会产生泡沫经济。与17世纪荷兰的郁金香泡沫、18世纪英国的南海贸易公司泡沫一样，自古以来都有泡沫这个概念。但是日本的泡沫经济崩溃，并不能全部解释为简单的过度投机，同时也是日本的社会经济体系在进入全球化的进程中被批了一个“NO”，不能被全球所认同。仍以上述的生态体系为例，可以说日本因为距离欧洲大陆较远的原因，一直维持了独有的生态环境。但是一旦面向世界，就如同生态环境里面来了一条吃鲇鱼的外来的黑鲈。

另外，泡沫作为一个“泡”，并不是只有幻灭一条路。1999～2000年，美国随着硅谷化的发展形成了IT泡沫和上市狂潮。但是，伴随着因特网的急速发展，IT企业集中了大量丰富的资金并以股票期权吸引了高水平人才。这种力量摧毁了(一部分)既有的经济业务流程，产生了一些(在IT泡沫破裂以后仍然生存下来的)新的商业模式；而从贴近我们生活的角度说，工作中的商务休闲装也逐渐流行。这一切改变了世界，整个产业旧貌换新颜。

日本的泡沫时代，要不是被世界/美国说了“NO”，说不定城市中心一等地价区内将会建造200层以上的超高层建筑之类，使得高涨的土地价格一部分得到回归。实际上，的确也听说当时有大型的房地产建筑开发公司

已经在制订2 000米高的高层建筑计划了。

泡沫经济破灭后，为了形成新的经济生态系统，日本社会须渡过重重难关，因为单独任何一个要素的变化都会引起相关要素的连锁反应，所以日本社会苦难重重在所难免。但是最近，企业逐渐有所盈利，正在朝良性发展。

中国经济在改革开放后得到了持续稳定的增长，首先获得发展机遇的是出口制造型行业，中国也因此被称为“世界工厂”。2001年中国加入WTO后，几乎可以被称为是“世界市场”，成为影响世界经济的一股巨大力量。例如，中国目前手机移动用户数量已居世界第一，2007年使用因特网的人口超过1.3亿，仅次于美国居世界第二。此外，一般认为世界能源及原材料价格的高涨的一个重要因素就是中国需求的增长。

中国的企业在这样的环境下也加速了自身全球化的进程。一方面在与国外企业或国内外资企业的竞争中修炼内功，另一方面也在不断地吸取世界上最佳实践的经验。相信中国企业在各个领域成为世界领军企业的日子指日可待。

在中国，2003年随着国资委的成立，国资委以国有资产的保值增值为目标，不断地采取鼓励兼并、明确一把手的考核机制、强化法人治理的一系列手段，逐步地把国有企业打造成为中国经济的一股中坚力量。目前国有企业所主导的国有经济对GDP的贡献率约占30%以上。改革开放后，作为中国经济的第二支重要力量的私营企业蓬勃发展，推动了中国经济的发展，据最新的统计，其对GDP的贡献约在40%以上。除了这两者，就是俗称为“三资企业”的第三支经济力量，即外商独资企业、外商合资企业和中外合作企业，它们对GDP的贡献在20%左右。

可以说目前中国经济的一大特色就是，企业行为和员工对待就业的态度是以经济的高速发展为前提的。

步入2008年，由于现行汇率机制的不健全，导致境外热钱大量涌入，挤占国内资产而导致的外向型通货膨胀非常显著。中国政府已经动用了在传统西方经济学中几乎所有的利率和汇率工具来抑制通货膨胀。但随

之产生的副作用是不断升高的利率导致企业的生存空间日益艰难，而不断攀升的汇率更是对所有外向型出口企业带来了重大影响。而这其中很多都是私营企业和三资企业，国有企业受到的冲击相对小一些。这个结构性调整的痛苦过程将需要一定的时间才将会最终完成。

以下是笔者对于中国私营企业的分析，该观点仅仅是在与美日情况比较之后得出的个人意见，仅供参考。

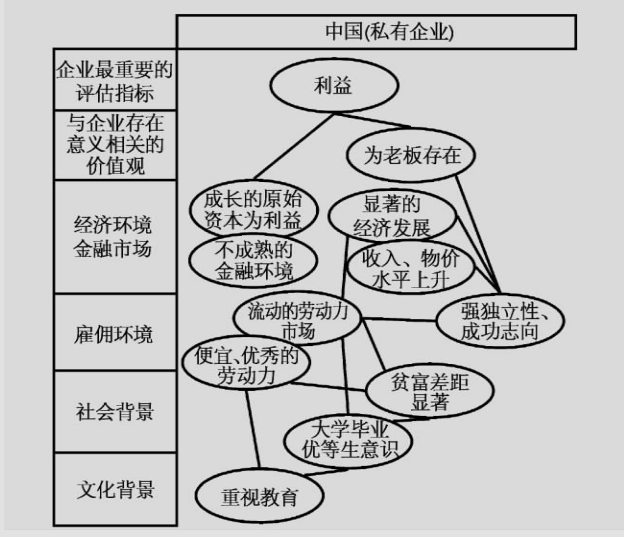

图 2-2　企业所处环境要素之间相互关联的示意图(中国)

这样，最终回到内部控制的话题，“控制环境”这个概念，把前文提到的所有要素均包含在内了。“内部控制”是来自美国的全球化运动的先行理念之一。在企业内、外部均变化如此巨大的时代，笔者想也没有任何一个经营者敢断言“其公司内部管理制度无需进行改善”。

第三章　销售(2)：收入确认、催款、收款

通过运用信息系统，提高业务与内部控制水平是所有企业的课题

应收账款：谁都可能被虚增销售的诱惑拉下水

美国的安然事件、世通事件，日本的嘉娜宝事件以及中国的银广夏事件，都与虚假记录巨额销售收入有瓜葛，收入确认是现今内部控制要点的重中之重。确认收入是公司利润的来源，管理层凭一己之力轻易就能操纵产生大额销售。而且，不只是管理层，子公司的总经理、部门主管，甚至是业务员，在迫于各种压力之下，都有可能在任何时候受利益驱使，进行虚增销售收入的操作。从外部审计人员的观点来看，“收入确认”也是审计的重点之一，需要投入更多的时间进行审计。

从内部控制方面来看，与收入确认相关的最关键的控制是针对收入确认的标准进行明确书面规定，并妥当制作、获取、保管，作为收入确认依据的相关凭证。

“所有权及和所有权相关的风险合理地转移至买方的时点”是收入确认的基本原则。从这个意义上说，收入确认时点是以购销合同上规定的条款为准。在中国，实务上也大多根据原则重视合同条款，有购销合同时

依照合同，没有合同时以买方确认验收入库为准的情况较多。但是从实务角度说，国外许多公司确认客户验收入库时点往往滞后，但更易把握自身的发货情况，而且由于国内送货途中的运输问题较少，因此从习惯上大多以发货时点为收入确认基准。但是当公司客户群固定，而且双方之间能够通过信息系统进行直接的数据交换时，将客户验收入库作为收入确认的基准是更加适当的。

在设备制造以及销售的行业中，有依照合同以出货时点作为收入确认时点的，也有以按照安装完成后作为收入确认时点的，另外还有先给予客户试用再确认销售等各种复杂的情况。这种时候就需要从“所有权及和所有权相关的风险合理地转移至买方的时点”的原则出发分析业务，根据收入确认的基准，妥当保管好相关凭证。

进行出口销售业务时，一般以单笔业务的国际商业贸易条款为依据作为收入确认的时点。母公司管理子公司之间的买卖时，根据不同的贸易条款，出口方应该等到从进口方传回单据后才能确认收入，但是由于后面章节讲到的提前结算的影响，必须要考虑可能漏记销售的情况。

此外，针对收入确认是否适当，应该尽可能成立独立的部门定期检查。具体讲，就是对入账的收入进行抽样，确认作为收入确认基准的凭证以及数据是否存在、收入确认时点是否确切，同时检查下期初、月初有无非正常的退货。因为在期末记入销售收入，但在下一期期初再退货，以此虚增收入的做法，是一种常用而又经典的虚假记入收入的手法。

这些程序在外部审计当中是通常会使用的审计方法。由于收入确认的重要性，建议将该做法也作为公司的内部控制，并予以实施[1]。

开发票：该业务流程在不同国家，区别巨大

开发票(Invoice)以及收款，各国的商业习惯上有很大区别。

中国开发票的实务操作，与其他国家有着很大的不同，其流程有其独

特之处。

无论是根据旧会计准则或者根据 2006 年财政部颁布的新的会计准则，销售并不是在开具发票之后才进行确认的，必须按照权责发生制的原则，确认销售（以及应收账款和销售成本）。这点是经常容易被混淆的概念。在确认销售同时，应该及时开具发票；但实务中如果未能及时开具发票，在进行纳税申报时，都必须填入“未开具发票”一栏中进行申报，税务局的纳税申报表上也有该栏。（进而言之，增值税也应该根据权责发生制的原则，当确认销售时应该同时确认增值税销项税额。）

在开具发票流程中，内部控制要求应该做到的是能够确保无遗漏地开具所有发票，为此可以针对开具发票申请以及财务记账凭证进行管理，并在开具发票之后对已开发票内容再做双重检查，确认有无盖上发票专用章。

然而，在与政府机关或者医院等进行往来交易时，一般先收到货物，支付货款完毕后，对方才开出发票。前面章节中也曾提到过，在中国国内，一般的企业间进行交易时，部分采用预付货款，在确认货款入账之后再进行发货并开具发票。发票只有在授信交易中，起到催付货款的作用。

在其他国家，开具 Invoice（付款通知书）时，只是将请求付款内容打印在普通的纸张上，和一般的订单形式差不多，是为了催促对方付款，与销售确认和税金无关。而且如要进行修改或者取消（开具 Credit Note），操作也很容易。

由于在很多行业中，付款通知书上的价格、付款条件、订单条款等项目与订单信息完全一致，实际上其就是根据“得到确认的（系统内部保存好的）订单内容”自动打印而成。总之，信息系统中用到最多的功能就是自动校验。反之，对于因频繁调价、订单内容和付款通知内容常常不一致的行业来说，在发出付款通知书以前，如果不经过盖章查看是不可能放心的，于是，这些行业往往在发出付款通知书之前会对其进行检查和批准。

总之，关于检查付款通知书的内部控制关键点是“付款通知书上的价格、付款条件是否正确，是否经过审批”。虽然中国的发票和国外的 Invoice（付款通知书）本来起到的作用各不一样，但是内部控制对于其基本

要求是一样的。

除上述所讲的之外，各国在开具发票(Invoice)以及确认应收账款流程中，主要有如下几点不同。

(1) 收款条件方面。欧美多是卖方在付款通知书中明确指定付款日期，一般使用的支付条款也只有几种到十几种。而与此相对应，在日本，一般配合客户的情况有多种选择，客户月末结算的就在次月的某日支付，或者 15 号结算的就在次月末支付。在中国，采取先预收货款的交易模式比较多，当给予客户授信额度时，一般是要求对方在收到发票/付款请求之后1～3个月内进行付款。

(2) 发出付款通知书的时点方面。欧美基本是只开出一份随货的单笔业务的 Invoice，中国也会按照一笔货物开出对应发票。与此相对应，在日本大部分公司到月底也会另外发出正规的月度付款通知书。

(3) 支付方式。在欧洲和日本基本以银行转账进行支付，然而在美国仍经常使用支票，委托外部有效率地进行收款。在中国，在进行大额国内支付时，基本上都使用银行转账进行支付，只有在小额采购时会使用转账支票。而据说意大利因建有全国共通的结算体系，支付方式又有所不同。

(4) 对于延迟收款的确认。近年来，虽然日本企业和中国企业也开始导入欧美开发的集成化管理信息系统，对公司单笔业务出货确认应收账款，收款后单独进行核销 狙是仍有企业根据应收账款余额进行收款核销。

▼ 对确认收款延迟的讨论

针对上述(4)确认收款延迟的问题，笔者之前曾与一位丹麦的会计师进行过探讨。这位丹麦会计师认为，对于将总的收款金额与应收账款余额进行核销时，会产生如下问题：

- 在应收账款账龄表(应收账款销账后余额表)中无法正确显示该笔逾期应收账款。
- 不能明确该笔货款究竟逾期多少时间(对每月的应收账款余额整体进行核销时，只能了解每月应收账款的欠账额)。

上述案例(见图 3-1、图 3-2)中公司的信息系统是日本式的集成化信

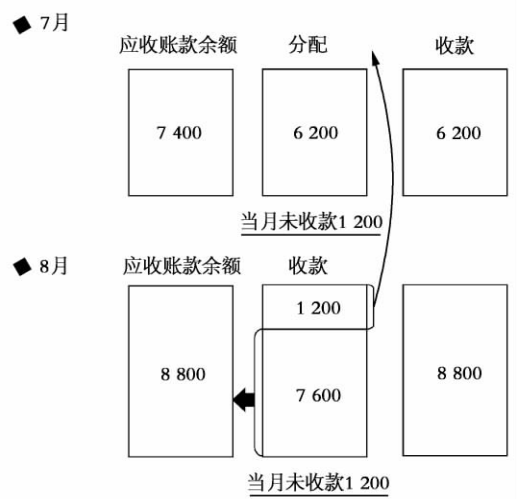

图 3-1　月度应收账款余额收款时的核销

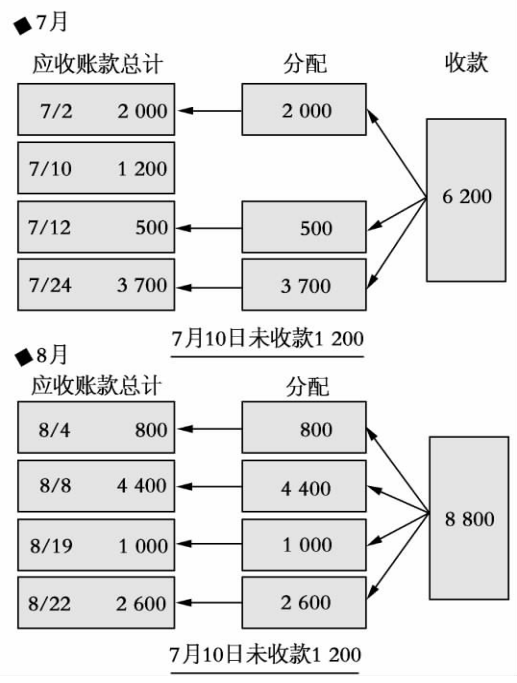

图 3-2　以出库为单位计算的应收账款的收款核销

息系统，只能按将每月总的收款金额来核销该月的应收账款余额，那么如果要满足这位丹麦会计师的要求，系统必须换成具有针对单笔业务进行核销功能的系统，或者对现有系统进行大规模的修改[2]。

这样，管理信息系统对于业务及内部控制都影响巨大。另外基于日本(或中国)的商业习惯而形成的业务模式以及内部控制，由于其与国际惯例不同，也往往不被认同。除上述例子之外，还有很多，不胜枚举。

并且，即使认同接受了这种以收款总额来核销应收账款余额的做法，并将其在业务流程以及内部控制中予以运行，但按照单笔出货来进行应收账款核销的方式，从管理角度来看更佳。

▼ 业务流程的处理速度及质量

过去，业务流程中，每月处理一次的工作较为常见。如每月一次制订销售、生产计划，落实库存、调配计划，月末财务编制科目余额表等。如今，人们越来越多地要求以更高的频度对计划等进行修正或处理，但是仍然还有很多企业对于各种业务维持每月一次的处理方式。

比如近年流行的供应链管理，通过该系统，将原本每月处理一次的业务，提速到每周一次、每天一次，甚至随时进行，其主要目的就是尽量减少业务流程从头到尾各环节的处理时间。如果没有网络和高度发达的信息管理系统，也不会有今天的高度商业化。

同样在会计行业，每季度决算的常规化和每月决算(并非科目余额试算表)的实施也是向同一个更实时的方向发展。其处理速度以及质量，受信息系统的运用是否到位和相关业务流程的设计是否合理的影响，最终结果可能千差万别。

早前听到某个美国企业，在年度末之后 3 天内就完成了年末结账的工作。而且该公司的结账不仅是其单体，而是整个合并报表。

如前述的有关开具发票和确认销售，通常的做法是每天开票，并且据此确认销售，然后只要每月一次核对本月实际发生的交易和开具发票的金额就足够了。但是这种做法仍有欠缺。如果财务会计系统能够自动与

开票系统进行衔接，将销售数据实时地导入开票系统，自动执行开票的话，业务效率会更高，而且不用考虑月末执行人工核对，减少了出错的可能性。

灵活运用信息系统以提高业务流程及内部控制的水准，应该是所有企业的必修课。

收款：能否信赖信息系统是个大问题

从业务销售实务的角度来讲，接到订单当然是最难的工作，在那之后的出货、开出发票、收款等程序可以说都是偏事务性工作的业务流程了。这样的工作如果能有效地运用信息系统，进行自动化、高效化整合是提高业务效率的关键。但是自动化系统尽管有利于内部控制的检验、检查等优点，也同时存在某些问题。

各行各业中，但凡一般的大型企业都会将收回货款与应收账款进行核对，然后考虑银行手续费造成的减额、折扣、到期日前的收款等种种因素，对应收账款进行核销。如果该工作完全依赖于手工作业，将是非常大的工作量。在中国国内，仍然有很多企业依靠手工作业来进行应收账款核销 国外的大型企业中，大多在信息系统中设定一定的条件自动进行应收账款核销工作，只有在实在核对不上的时候才由分管收款的人员会同销售业务员一起调查原因。

自动进行核销应收账款的首要前提是需要设定一个放宽的金额，例如预计的银行手续费等，假设为 30 元。当收到货款与应收账款余额的容许误差在设定的 30 元之内，则自动执行应收账款核销。

在欧美，很多公司为了提高工作效率，一般都将这个容许范围设定得较大。听说某英国公司，从新客户处收到第一个月的收款金额与应收余额有差额，但金额不大就没有向客户深究。但第二个月收回的货款与应收款的余额仍然存在差额，且比第一个月还要大，第三个月的差额索性更

大。于是,公司和客户进行了沟通,结果第四个月的收款差额还是和第二个月的差额持平。虽然这也算不上是舞弊,但称得上是由于信息系统自动化产生的控制盲点的一个例子。

▼ 系统登录权限的限制是个重要的控制

对于这样依赖于信息系统的业务流程来说,其内部控制流程只能建立在完全信赖信息系统的前提之上。

即使一个系统功能十分完善,如果任何人都有权限登录并能够修改其内容,其风险也是很大的。或者是一个系统的开发维护不到位,系统错误泛滥,在该系统中就无法保证相应功能的实现,包括诸如"依据经过批准的订单内容毫无更改地自动生成发票";"根据发货数据正确记入收入、应收账款"。

销售循环中的舞弊行为,比如减少应收账款余额,将减少的金额与客户平分,或者截留收到的货款,等等,这类行为只要适当地设置系统登录权限,就能较大程度地遏制类似的舞弊行为。

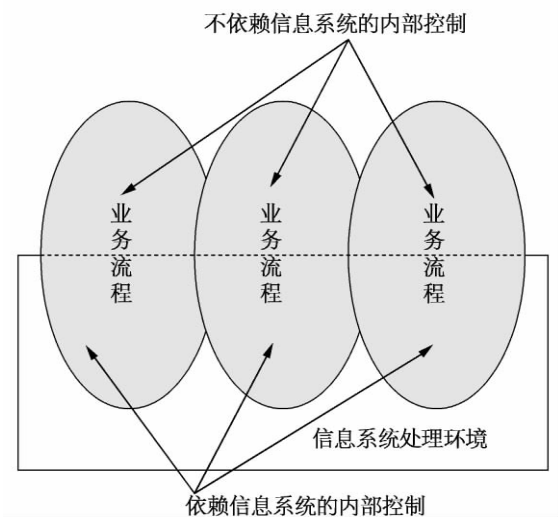

图 3-3　信息系统和业务流程中内部控制的关系

诸如如何确保信息系统是能够信赖的，我们将其称为“信息系统的整体控制”。

客户、供应商的主文档：对于主文档的控制是防止舞弊和失误的最后一道防线

主文档是指在信息系统中事先登记录入的基本情况。比如客户主文档就有客户名称、客户收货地址、付款通知寄件地址、客户的业务人员名称、结算条款，还可能有信用额度，以及会影响销售价格的该客户分类等。另外在这里值得一提的是，供应商主文档中，可能包含和付款相关的具有很高风险度的信息，如付款银行账号等。

主文档的数据，由于在制作、处理单据时每次都会被引用，并被核对，因此保证主文档内容的正确性是非常重要的。另外，针对客户、供应商主文档，会由于管理不善，造成不正当利用和产生成批错误，风险是很大的。因此，切实有效地管理好主文档是防止舞弊及失误的最后一道防线。

关于供应商主文档，采购方虽将材料和商品的供应商单独登记在主文档中，但是发生零碎繁杂经费，面对这些小的服务供应商时，就笼统地在系统主文档中虚设一个公用户（杂项），这种管理是非常不理想的。从内部统一管理的观点出发，事先未有效地登记供应商信息意味着每次付款时（各担当）都要一一输入供应商的相关信息，这必然伴随着相应风险的产生。同时，也可能在各项统计中发现“本公司本部门交易量最大的供应商竟然为杂项”。所以，应尽量避免使用诸如上述的“杂项”供应商设置，而是根据明文规定来进行操作，严格管理。（夸张地说，为招待客户应酬而定点的饭店都最好能够设置相应的供应商主文档。）

登录客户、供应商主文档以及变更主文档，都应经过适当的管理者的批准才能进行。批准登记主文档信息可以和新客户或新供应商的批准同时进行。此外，登录、变更主文档内容之后，最好由实际操作人员以外的人再对主文档进行核对。

在内部控制中更可能常常产生问题的,就是对客户、供应商主文档未进行定期复核。为什么说这个会成为问题呢?因为实际上很少有企业能够做好这个工作。当客户和供应商数量众多时,从实务角度来看,定期对主文档的内容一一进行确认,确实比较困难;再加上如前述的对费用付款方要求也单独登记的话,定期对主文档的复核更是难上加难。

但是,要是抱着"登录变更之后再确认也可以"、"每天制作票据时都会引用相关内容,到时候再确认也不晚"这样的想法,是非常危险的。当负责登记、变更的操作员在录入批准后,又故意对已录入信息进行更改,或者存在长期未使用的主文档信息时,款项被汇入了已破产的供应商的银行账户,这种舞弊行为的后果不堪设想。

实际上,当一一复核每一项主文档信息很困难时,可以让系统自动统计打印出一定期间(前次复核开始至这次复核期间)的信息新增变更内容的报告,只对新增及变更部分进行复核。另外也可以通过程序实现以下功能:对于一定时期没有使用过的客户或供应商,系统自动对其主文档信息进行冻结或者删除,像这样借助系统的力量代替人为内部控制也是可行的。但是每种方法都由各自的优缺点,应该结合实际,考虑选取最适合的功能及控制流程。

注

[1] 内部控制通常是为了确保能够产生正确的数据而形成的系统。但在这里针对的销售收入财务记录的复核,是对记录的数字金额进行抽样,和外部审计的程序完全一样,也许大家会稍许有点疑惑,为什么要求企业执行外部的审计程序。的确在内部控制程序中,即使是有些外部审计程序相当重要,单作为内部控制,一般并不被采用。但是正如正文所讲的,因为销售收入记录的重要性,建议公司的内部控制程序也一定程度上实施外部审计的程序。从学术上来讲,这种程序与外部审计相近,不是业务流程层面的内部控制。从内部控制要素

的角度看，这不属于“控制活动”，而是“监督”这个要素。

[2] 应收账款收款核销原本是公司必须作出判断的工作。当公司未能完全收款，不能进行核销时，与付款方进行确认才能知道付款方的意图。也有可能是由于对方手头资金不足，而未能付足全部货款。因此，调查逾期应收账款是一项非常重要的内部控制工作。

第四章　采购(1)：内部控制的原点

为了确保“公司健全的构造体系”，而不断进化的内部控制

内部控制的产生和发展：美国萨班斯(SOX)法案、日本版 SOX 的导入是广义内部控制的胜利

Oh When the Saint ～♪ Go Mar-Chin'In ～ ♪

Oh When the Saint ～ Go ～ Mar ～ Chin'In ～ ♪

Load I Want ～ to be ～ in that Number ～ ♪

When the Saint ～ Go ～ Mar ～ - Chin' ～ In ～ ♪

“圣者的前进”是一种最古老的迪克西兰爵士(Dixieland Jazz)音乐的代表作。20 世纪初在美国新奥尔良把爵士乐确立为音乐类型的时候，内部控制的概念也得到了确立(1900～1910 年左右)。

当时内部控制的焦点是现金、支票的管理，以及与之相关的支付处理。内部控制的原型是‘防止与现金、支付相关的舞弊行为的架构’，因为当时代表性的舞弊行为是员工私自花掉了现金，或是下一番工夫掩盖不正当的支付等行为。

从 1910～1920 年，西方列强为富国强兵，飞速发展重工业。随着企

业规模的扩大，内部控制的概念得到发展，蜕变为“确保构成财务报表数据的每笔业务是否都得到正确执行的架构”（这段时间爵士乐中心转移至芝加哥发展出了摇摆爵士乐（Swing Jazz）音乐）。

随着企业依靠银行贷款或者从股票市场融资的普及，财务报表作为对企业进行评估的资料，其重要性的凸显是一个很大的原因；另一个原因就是由于企业规模的扩大，审计师对公司所有的业务进行验证变得愈加困难，这样审计师需要有一个不对全部业务进行检验就能完成审计工作的理论。也就是说，“首先确认业务是否被有效地管理，比起直接验证每笔业务要有效率得多”。

这个概念成为（美国 SOX 法案和日本版 SOX 公布以前的）对内部控制实施评价的理论依据，即在每个会计期间的期中对内部控制系统进行评价，在此结果的基础上决定期末余额审计必需的样本数量，通过合理的确证使工作最有效率。

▼ 广义的内部控制及狭义的内部控制

第二次世界大战后的 1949 年，美国发表了美国审计程序委员会（American Institute of Accountants，AIA）的特别报告书，将预算、统计分析、标准成本、员工培训计划等与财务、会计处理不直接相关的事项都包含进了内部控制概念中。内部控制的概念进一步得到了扩大（这就是所谓的广义的内部控制）。

与此相对的是，主要的会计师团体在 1940～1950 年发行的《案例研究及审计》手册中，将需测试的内部控制的范围限定为会计控制。审计师所了解的、同时需要验证的是和会计处理相关的业务，范围进一步扩大会给审计师带来很大的困扰（这就是所谓的狭义的内部控制）。

但是，到了 1950～1960 年，由于环境问题等，企业的社会责任进一步扩大，对于应该最了解企业情况的外部注册会计师，社会赋予了他们更高的责任，要求其超越原来验证财务报表数字的职责，做到“对企业内部控制进行全面的把握”。

1970年代，注册会计师由于管理层粉饰报表的行为而被追究责任的案例不断出现，1988年公布的审计准则公告55号(SAS55)中明确指出，作为审计程序的其中一环，外部审计人员有义务了解公司内部控制的构造，并对风险进行评价。

另外，1976年发生的Lockheed事件，是美国的知名企业向日本、荷兰、墨西哥等国政府高官行贿事件被曝光，并且造成了日本当时首相辞任的重大事件，在美国也造成了很大影响，内部控制对管理层行为的监控是否有局限成了问题的焦点。内部控制本来是由业务流程层面的内部牵制发展而来的，所以的确可以说是有局限的。

将上述发展过程综合起来的是1992年公布的美国COSO内部控制整体框架报告(参看第一章注释1)。这里定义的内部控制框架是在最初的控制活动(业务流程层面的内部控制)基础之上，增加了控制环境(公司管理及企业文化)、风险评估、监督(内部审计的机能)、信息及传达(信息系统等)等内部控制的要素而形成。可以说，内部控制的概念也由此进一步发展成为了“确保公司健全的构造体系”。

另外2002年美国企业改革法(即萨班斯法案，美国SOX法案)，将原来只作为财务报表审计的辅助程序的内部控制评价一举提高到准主角的地位。就受美国证监会(SEC)监管的在美上市企业而言，管理层有义务对财务报表的公正表述和内部控制的有效性宣誓负责。同时，外部审计师除了出具针对财务报表的审计报告外，还必须出具针对企业内部控制有效性的审计报告。

但是，美国SOX法案和与其相伴的SEC规定都限定了“对财务报表产生影响的”内部控制，从这一点继承了狭义的内部控制概念。由此，我们将其称为“准主角”。

▼ 比较一下舞弊行为的内容

这里，让我们回到20世纪初，内部控制概念形成之初的中心是现金、存款的管理及支付程序。从那时算起，正好是在100年后的2002年，制

定美国 SOX 法案的契机却是针对舞弊行为，比如管理层粉饰决算、虚增利润和销售额等，这是不是一个非常有意思的对照呢？见表 4-1。

表 4-1　1900 年代与 2000 年代舞弊比较表

	1900～1910 年	2000～2004 年
具有代表性的舞弊	诈取现金	粉饰决算
舞弊实施人	员工	管理层
相关会计科目	现金及银行存款、应收账款	利润、销售收入
内部控制的焦点	现金及银行存款管理、支付程序	公司层面内部控制

与采购循环相关的内部控制的原型：内部控制的原点是采购和支出的检查和控制

说到 20 世纪初的美国，公司规模还很小，还没有 IR（投资关系）的理念，连信息系统的影子都还没有出现。介绍一下作为内部控制原点的采购循环在那个时代的真实情况是非常有意义的。

下面列举的未必是上世纪初企业情况的忠实再现，但都是采购循环中重要的内部控制行为的原型。

- 采购申请部门，填写请购单。
- 采购部门批准请购单内容，制作订单，在传送给供应商的同时将其中的一联交于验收部门和会计部门。
- 验收部门验收实物后，把从供应商处收到的货物与订单联相对照，确认无误后收货，填写入库通知单交给会计部门。
- 会计部门负责应付账款的人员收到从供货方传来的发票（Invoice），在与订单及入库通知单对照无误后装订到一起。（凭证）
- 会计部长（Controller）在记账凭证上盖付讫（VOID）印章，交付财务部门。
- 财务部长（Treasurer）[1] 确认盖好 VOID 印章的凭证内容后，签署支票送交供应商。

· 会计部门负责银行余额调整的人员进行银行余额调整。

希望大家从中可以明白这样控制的目的：使单独一个分管人员、管理者或者一个部门、即使是会计或者财务部门的负责人也不可能轻松地实施舞弊行为。特别是账簿和实物(支票)是分别由会计部门和财务部门管理的，这是职责分工的一个要点。假设财务部长不正当地签发了支票，由于和会计部门掌管的账簿记录不符，在银行余额调整时就能被发现。而会计部门之前填写、处理的凭证，都会经过后续部门的检查对照。

在交易频繁、信息系统发达的现代社会，仍保持像上文那样的内部控制行为的公司当然已经没有了。但是在欧美企业，尽管在形式上多少有些变化，但还是基本遵循了以上原则。

日本大部分的企业没有遵循这些原则，与其说是因为利用了信息系统或者为了提高效率，不如说多数时候仅仅是因为假设了“员工不会发生舞弊行为，或者管理者不可能舞弊”的前提。比如说会计和财务的职能分工，就算是很大的企业，不明确、不充分的情况也很多。我们当然还是希望分别设置会计部门和财务部门，如果不是这样，至少出纳和账务记录人员必须要明确职责分离。

在中国，财政部 1996 年颁布的《会计基础工作规范》明确记载了出纳和会计工作分离的必要性。这一点是被广泛认同的，但会计部门和财务部门的分离还不是那么普遍。此外，特别是私营企业，老板往往会亲自确认每一笔支付，做成它的内部控制。上述例子中的职责分工往往有得不到重视的倾向。

正如第一章中讲到的那样，控制环境正在不断地发生着变化。因此，我们必须认真考虑建立适当的架构体系，使采购和支付相关部门的分管人员或管理者即使有舞弊的念头，也不可能单独地完成，或者当发生舞弊行为时能够及时被发现。

注

[1] 中文中“财务”一词指 Financial Accounting，也包括了会计业务。本文中笔者提到的财务部门和会计部门的分离，是将财务部门认定为主要负责资金管理（Treasury）的部门。

此外，日语中的“财务”仅指资金管理（Treasury）这一狭义概念，与中文的财务相对的词语是“财务会计”。有趣的是，日语中“经理”一词与中文的“会计”是同样的意思，日本大部分公司的会计部门都称为“经理部”。

第五章　采购(2)：下单、请购

所有的采购行为都必须获批准

业务循环：关键是以哪个业务循环为对象

本章的主题是采购前半部分的下单及请购。在采购循环中，不仅包括了原材料、零部件的一般意义上的采购，还包括了外包加工费、水电费、交际费、广告宣传费、销售手续费等（工资和税费除外）所有和支付相关的业务流程及与之相关的内部控制。

提到广告宣传费和销售手续费，有人可能会问“这个不是应该属于销售吗？”这里，首先让我们来看一下业务循环的概念。相对于业务流程（一系列业务）这个一般术语，“业务循环”是考虑与财务报告相关的内部控制时的一种划分方式，包括生成相关会计科目数字的一系列业务流程。

其他的会计师事务所或者一些辅助设计内部控制的软件工具中也许并不使用‘业务循环’这个字眼，即便如此，他们也一定会关注各主要业务流程与哪些会计科目相关联。

日本版 SOX 中，与采购循环相关的商品和原材料的购入通常作为“与企业经营目标密切相关的”业务流程而成为一般评价的对象，而大多数的费用项目则不一定有必要作为评价对象。但是，由于行业的不同，比

如化妆品行业等，广告宣传费用甚至超过了产品成本，因此比起采购、存货循环来，也许有时候广告宣传费更值得评价。又如对于制药行业，研发费用可能就尤为重要。

而在美国 SOX 法案中，普通费用原本就是评价对象，但有时也会根据 AS5（审计准则第 5 号），按照风险导向的观点进行判断。

▼ 最能恰当说明的业务循环

像表 5-1 表述的那样，销售循环除了销售收入、应收账款以外，还有产生销售折扣、坏账准备金等与损益相关科目金额的业务流程，以及其中所包含的内部控制。与此相对应，采购循环则包括了各种费用的发生和支付。从业务的角度看起来多少有点不好理解，但是毋庸讳言，广告宣传费，以及与销售相关的运费、保险费、销售手续费等等，都是采购循环的对象。

表 5-1　一般的商业循环

业务循环名称	主要相关会计科目
销售循环 (Revenue Cycle)	销售收入、应收账款等
采购循环 (Expenditure Cycle)	销售费用、应付账款、应付费用、预付费用等
存货循环 (Inventory Cycle)	存货、销售成本等
固定资产循环 (Fixed Assets Cycle)	固定资产、折旧等
资金循环 (Treasury Cycle)	借款、投资、投资收益、利息费用等
人事薪资循环 (Payroll Cycle)	应付工资、应付福利费、退职准备金等
税费循环 (Taxes Cycle)	应交税费等

尽管这样,也有一些业务流程,很难将其归属到某个商业循环。比如说销售发生之时,“借:应收账款,贷:主营业务收入”这个销售循环的会计分录和“借:主营业务支出,贷:库存商品”这个存货循环的会计分录同时发生。同样,从采购方收到商品时的“入库”会计处理,也涉及采购和存货两个循环。

对增值税来说,也是销售时发生销项税额,采购时发生进项税额,在决算时相抵后向税务局申报。

总之,在考虑会计科目和披露事项的前提下,尽可能恰当地把业务放到内部控制业务循环中。

业务和内部控制模式存在很大差异时,可能对于同一业务循环需要进行多次文件化和测试的评价工作。比如说,存在“总公司采购”和“工厂采购”两种平行的业务流程时。另外,在金融行业和建筑行业等具有特殊会计科目的公司,也设有专门说明这些会计科目的独特的业务循环。

还有,固定资产的取得、清理、折旧都属于固定资产业务循环,利息属于资费循环,由此产生的应付款项及其支付通常属于采购循环。固定资产减值测试,可以作为固定资产循环,也可以作为决算及财务报告流程的一部分进行评价。

订单的批准:所有的下单行为都有必要经过适当的斟酌和获得批准

现在,让我们进入本章的主题——“采购”。

所有的支付(除了工资和税费),都伴随着下单的动作。也许交际费、销售手续费等费用并不使用“下单”这个字眼,但请从提供服务及发生与之相对应的付款约定的角度广义地进行理解。

采购循环中的所有下单行为,都有必要经过适当的斟酌并获得批准。这是与销售循环对照而言的,销售循环的“接受订单”,只要在许可的价格和信用额度内,从内部控制的观点出发,没有要求对收到的个别订单特别

关注。除非是有特别幸运的公司，否则从客户那里取得订单都是很不容易的工作。反之，向供应商下订单则是很简单的事情，公司的审查和预算只要稍有松懈（而且只要是公司出钱），立刻就会想到要解囊了，这也是人的本性吧。

由于这种原因，“下单”是容易产生舞弊行为的业务之一。从业务层面来看，这是一个需要常年对其适当性进行斟酌的业务流程。我们也能看到一些例子，仅仅是不当花费了几万元就导致了企业的重大丑闻。

说到采购的批准，像巨额采购和附带特殊条件的协议，需要经过书面请示或通过经营会议讨论同意等特殊流程；而类似交通费、办公用品采购等则可以通过诸如事后汇总报批的简单流程来处理。在框架合同中约定价格和数量的上限，数量和交货期则通过个别订单来实行的情况，框架合同当然要得到负责人的批准，而个别订单视权限规定等情况则可由担当的业务员来判断定夺。

对于组装生产企业，有时材料需求计划系统（MRP）中各零部件的需求数量被直接转发给供应商实施订货。在这样的情况下，我们可以认为对产品生产计划的批准可以视同对订单的批准。

订单的形式虽然千变万化，但万变不离其宗的是，下订单时至少要对价格、供应商、订货数量、用途及交货期等进行斟酌。

不同采购模式下的采购内容及审批要点见表 5-2。

表 5-2　各种采购模式中主要的采购内容及一般审批要点

	缔结框架合同的模式	MRP 下单的模式	个别采购且使用采购申请的模式
品种	框架合同或订单	基于生产计划的需求量	采购申请
数量	框架合同或订单	基于生产计划的需求量	采购申请
供应商	框架合同	（一般为）框架合同	个别合同
价格	框架合同	（一般为）框架合同	个别合同
交货期	订单	框架合同、需求量	采购申请

订货申请部门和采购部门的分离：采购功能的设置从经营角度出发也是个重要课题

在采购的内部控制中，最重要的是订单或者个别合同的审批，其次可能就数“采购申请”了。

内部控制局限性中最有代表性的例子之一就是采购环节中的“内外勾结”，也是风险最集中的情况。极端的例子是，甚至有管理层亲自长期向供应商实施不恰当的订货而拿到巨额回扣。在这样的案例中，“管理层亲自”这一部分，就是被称作“管理层越权”(Management Override)，而这也是内部控制的另一个局限。

将采购申请部门和采购部门相分离，是为了降低这种如内外勾结等不正当采购行为的风险。具体而言，是将对外部下订单的功能集中于采购部门，需要物资或服务的各部门填写采购申请书交管理层确认购买的恰当性，批准后提交采购部门，采购部门从经济角度研究后再下订单的形式。供应商的选择虽然也可以考虑由需求部门提案申请，但原则上应该由采购部门决定。采购部门其实是总务管理性质的部门，该部门需要的基本上仅限于办公用品之类。

虽然在使用采购申请书的情况下，订单的批准、下单以及买卖合同一般都是由采购部门的管理者签名、盖章，但采购申请部门对于采购申请书的批准实质上实现了向采购部门管理者的权限转移。

▼ 集中采购的优势与劣势

采购功能的集中从业务层面考虑有以下优势：

- 全公司所有需要集中起来，订货数量可以成为价格谈判的筹码。
- 因为有采购的专门部门，就可以在经过充分研究比较供应商、价格以后再下单。

反之，采购功能的集中也有以下的劣势：

- 采购部门不熟悉特殊物资或者需要专业知识的物品和服务，无力对供应商、价格进行研究比较。
- 紧急／灵活采购和订货较为困难。

从固定资产到办公用品，基本都可以将其采购归并到一个部门。但是对上述劣势明显的特殊物资或服务进行采购的话，集中采购的形式可能不适合。

例如，商社（贸易公司）这种经营形态，它是由商品采购和销售并行的多个营业部门构成。营业部门并非单纯地从事销售，其工作内容还包括了在考虑销售机会和利润的基础上的采购行为。这样的情况，想将采购功能向一个部门集中和发出采购请求的概念就不适用了。可以想象，如果集中采购，那么根本就无法开展业务。但是，由于商社的经营模式是将采购来的商品直接卖掉以获取利润，一般说来利润率都相对较低，所以将商品以不当的高价购入以获取回扣的空间和可能性也较小。

因此，在探讨内部控制时，应该考虑具体的业务环境。依据这样的经营环境和状况（称作‘固有风险’），每种业务流程的内部控制应该根据实际的需要而变化。

▼ 保持适当采购业务形态的意义

很多制造业企业非常关注与采购申请有关的内部控制。包括集中采购在业务上的优势在内，适当的采购业务形态在企业战略层面上也具有很大的意义。

例如，日产汽车经营状况的扭转，据说成功的原因之一就是集中采购选择供应商，从而在短期内实现了采购费用的削减。此后，日产在重新考察选择供应商的基础上，与选定的供应商构筑了长期合作关系。这是建立并保持适当采购业务形态的一个很好的案例。

采购功能的集中，在日本也是个普遍的概念。但是对日本企业大多以工厂为单位集中，欧美企业常常是集中全公司范围内的采购。这也可以认为是日本企业多数与供应商构筑了长期关系、共同提高品质和技术

这样所谓的“产业集群”的做法，适合比较分散的采购。

中国的许多大型企业近几年为了防止舞弊和规范采购流程，也有从分散采购向集团统一采购转变的倾向。

在制造业中，由于原材料和零部件的“品质”会对后续制造工序的不合格品率，以及对之后售出产品的退货率和投诉件数产生有很大影响。显而易见，这些影响是无法以“低价”来交换的。

另外，针对“交货期”，特别是像供应链术语中的“关键部件”那样不可欠缺且从订货至交货的时间又很长的部件，关键是尽量缩短其交货期。缩短交货期，尽早将销售趋势和需求预测反映到生产上来，这对于防止错失销售机会或产生不必要的库存堆积都具有决定性的意义。

像这样的采购中的深层意义，欧美企业并非不知道，但是不管怎样也容易在短期利益的压力下，看中集中采购的低价位。反之，在很多日本企业都能见到的“哪怕没有利润也要做最好的产品”的现象也不是一朝一夕就能改变的思维模式。而近年来被称为世界制造工厂的中国，原材料或零部件的采购方可能更为强势，既追求低价位，又要求高品质的现象较为普遍。

就笔者看过的很多公司来说，制造部门和采购部门关系不融洽的问题，在东西方基本都是一样的。在对公司总体的目标、指标进行分析斟酌的基础上，为实现目标构筑一个“不是部分最优，而是总体最优的业务流程以及相应的内部控制制度”是非常必要的。

第六章　采购(3)：核对发票及支付

必须考虑舞弊行为

本章要介绍的是业务流程层面内部控制的重点：支付及与其相关的控制。第四章已经说过内部控制的原点是防止采购与支付流程中舞弊行为的发生，我们再来看一下当时所举的内部控制原型（20 世纪初）中，发票（Invoice）核对之后的动作。

- 会计部门中负责应付账款的人员收到从供货方传来的发票，在与订单及入库通知单对照无误后装订到一起（凭证）。
- 会计部长（Controller）在记账凭证上盖 VOID 印章，交付财务部门。
- 财务部长（Treasurer）确认盖好 VOID 印章的凭证内容后，签署支票送交供应商。
- 会计部门负责银行余额调整的人员进行银行余额调整。

让我们来比对上述流程，展开探讨。

发票核对：没有按照原则的情况很多

会计部门必须将①采购方送来的发票、②订单的复印件、③验收部门的入库报告这三类文件进行核对。这一核对工作是确保会计部门能够将正确的应付金额通知财务部门的重要行为。

然而,由于各种各样理由而没有按照上述原则实施的情况很多。

以下介绍一下核对工作中可能存在问题的例子。

▼ 例 1 根据发票记录采购

在销售(2)中也已经提起过,发票的发行由税务局负责,这是中国的发票形式在税务上和会计上的处理要点,也是世界上较少见的例子。发票成为管理的要点,同时严格执行付款请求的核对和凭证交付、保管的情况很多,但有时在采购环节也能看到因过于重视发票,本来应该实施的会计处理没有得以实施的情况。

实务中最常见的问题就是实施了购货入库验收,但是发票还未到时,不进行入账处理的情况。较多的公司都会按照销售的确认标准正确地实施会计处理,但对于采购的入账,很多情况下都会以收到发票作为确认采购的时点。

在会计处理上,应该以每次验收入库的事实为基础入账。实务操作确有困难的话,至少也应该在期末(上市公司的话至少是每季末)确认有没有已验收入库但发票未收到的采购并适时入账。

此外,在中国,在采购确认的时点一次记账的情况较多,但其他国家有在验收入库时和收到付款通知书时分别做两次分录的情况。

例如,导入 ERP 系统的公司在验收入库时也会使用"应付暂估"或者"GR/IR account"等暂挂科目,在对照付款通知书时借记该暂挂科目,贷记应付账款。

▼ 例 2 核对工作不是由会计部门,而是由其他现场部门实施

大公司中,如果将所有发票汇总到会计部门,那将会是巨大的数量,因此从合理化观点角度,在日本有时会见到由现场部门实施发票核对的情况。在中国,通常是现场部门在实务中将纸制凭证交给财务,由财务保管。这之中又有两种情况:(1)现场部门(通常是采购部门)把发票交给会计部门,由会计进一步进行核对;(2)现场部门将核对完的发票和采购订

单(甚至有时还包括入库单)交给会计部门。

这样做的原因之一是:发票内容是否正确可能只能依赖现场部门(如采购部门)进行判断。另外,在日本这样操作还有一个原因,就是由于供应商按月开具发票的情况很多,哪些采购应该当月开具发票,只有现场部门才能进行判断。

但是,是否原本就是适当的订单,应该在采购流程中判断,而不是由会计部门在核对发票时再考虑。

会计部门在发票核对工作中应该发挥的检查功能如下:

- 发票金额与应付金额一致;
- 发票本身的真实性,没有伪造或篡改;
- 支付条件和采购方银行账户与事前登记录入的信息一致;
- 近期没有同样金额的付款要求(避免重复支付)。

因此,虽然发票核对是内部控制中非常重要的行为,由于从业务来看属于相对简单的工作,所以这一工作有时会被考虑移交给近年流行的"共享服务中心"(Shared Service Center)进行管理。共享服务的概念是将多个部门或集团公司中相同的业务在一个地方进行集约式管理以提高效率,会计、人事等职能部门中比较简单的日常操作事务经常会成为集约管理的对象。

"间接部门的瘦身"是多数管理层孜孜追求的目标,即使将应由会计部门完成的简单工作移交给现场部门,表面上也只是减少了管理人员,没有实际意义。从内部控制的观点来看,如果负责核对发票的人员与制作订单、批准订单、入库(验收)等的业务实施者是同一人或在同一部门,发生舞弊的风险就会增加。例如,上述的第(2)种情形中就容易产生职责分工的潜在问题。

此外,原则上应该由发票核对部门直接从供应商那里收到发票,以杜绝可能的篡改发票行为。

在中国,一般不会有篡改发票的情况,但如果发票与依据凭证有差异,我们经常可以看到大多数公司会根据发票进行处理。因为红字发票

和发票的重开比较困难，有时即使有一点差异，也只能根据发票进行处理。但是，如果收到与经济事实有差异的发票，而按照发票处理的话，会导致发票核对这一重要内部控制失效的风险，所以应该设置一定的标准，对收到发票的差异进行分析，并批准、记录分析结果。

▼ 例 3：仅将发票与系统中的入库数据进行比较核对

例 1 讨论了“何时”入账，例 2 讨论了应该由“谁”来核对，那么这里打算讨论的就是与“什么”进行核对。

我们一开始就提到的 20 世纪初风格的“入库报告”中，一般只记载数量和品名；换言之，从订单数据中取得价格，从入库数据中取得数量，再计算要支付的金额并记账，将其与供应商开来的发票核对，这就是发票核对的原型。

在现代使用信息系统的企业中，将订单的复印件和入库报告以纸张的形式交给会计部门的情况应该不多见，验收部门等会将入库数量在系统中登记，然后由系统自动计算要支付的金额，并传送给发票核对部门。那么，是否可以不需要与订单核对呢？不可以。订单的核对对于确认入库及记账所依据的订单的真实性、牵制验收部门（以及应付款项计提部门）来说是非常必要的。

在中国，以纸张形式将验收入库凭证交付财务的情况比欧美和日本更多，有时与订单（数据）的核对比较马虎。

因此，除非信息系统能够很好地控制杜绝将虚假订单入账的情况，否则，必须对相应订单的真实存在性进行确认。

▼ 例 4：仅将费用发票或收据交付会计部门（无法核对）

费用通常没有“入库”的动作，那么应该与什么核对呢？

前面已经讨论了会计部门（发票核对部门）原则上应该做的是将“应付金额”和发票这一外部凭证相核对，并且确认订单或费用批准的真实性。费用的种类很多，处理方式也是多种多样，可能引发舞弊行为，因此

必须对发生的费用实施批准并确认发票与费用的性质相符。

首先，费用的发生金额，原则上应在事先经现场部门负责人批准。对于那些发生金额事先无法准确确定的费用，则应该先批准一个预计金额，事后再对预算和实际发生的差异进行批准。

会计部门（发票核对部门）应将该已批准的发生金额信息与发票核对。与物资采购同样需要实施采购申请及订单程序时，发生金额信息应该和记账金额一致，这个信息有时包含在经批准的采购申请书这样的文件中。

无论何种情况下，对于费用支出，其应付金额的确定（如果在物资采购中，则是由验收部门确定）和对该发生金额的批准（如果在物资采购中，则是采购部门确定）通常由同一部门实施，该部门必须将实际资料或记录于其他载体上的信息与发票进行核对，仔细检查发生金额批准的痕迹和外部发票的真实性和正确性。此外，用以核对的该两类文件应当由不同途径、不同人员向会计部门（发票核对部门）提供。

对于大额费用，建议也应该实施相当于入库（验收）的类似行为。例如，进出口的海运运费等发生金额经常达到数万元，如果全部检查很困难，可以考虑在抽样基础上或者对金额较大的部分获取港口的测量报告，再与发票内容核对。

对于广告宣传费，可以考虑通过抽样检查，或者委托专业市场调查公司的方式，确认与广告公司签订合同时确定的播放量，与电视广告中实际播放量是否一致。

反之，对于那些小额费用，可以由经办人将（已批准的）发票、收据交给会计部门。这时，需要互相核对的三类文件变成了一类。这种情况下，我们可以认为发生金额的批准行为是在事后，并且由费用发生部门连同发票核对的动作一起实施，会计部门仅实施会计入账。不过，由于这样的处理与职责分工不吻合，所以必须将其限定在一定的小金额范围内并明文规定。此外，还应该关注是否存在发票、收据‘没有’被使用部门批准的情况 如果有，应该作为极少的例外事项处理。

传统的会计部门应该对各现场部门的费用发生是否适当进行监控。

如此的监控角色非常重要。然而,正如例 1 中所提到的,笔者认为发票核对行为不应该承担如此高度的检查功能。“费用发生内容的适当性的斟酌”本质上相当于物资采购中“对发出订单的批准”,原则上应由发生费用的现场部门事前实施。

▼ 例 5:公司将“支付通知”发送给供应商,无需实施发票收到、核对的行为

在商业流程重组(Business Process Reengineering,BPR)流行的时期,制造业尤其是组装型产业已经大量采用这样的方式,即不是由公司将“应付金额”同供应商开来的发票进行核对,而是由供应商将“应到账金额”同公司发来的支付通知相核对。公司希望能够通过这样的流程来减少工作量。

在中国这样的方式还不多见,在一些日资企业的中国子公司可能会见到。

采用这样的方式时,需要讨论在内部控制上是否有问题,如果只采取发票核对,控制上还是有薄弱之处的。

首先,实施发票核对时,如果采购方的发票金额大于订单金额,那么一般会与供应商商议并调查原因;反之,如果发票金额小于订单金额,则可以先放任不管(当然,最终这也应该进行商议,调查)。与此相对的,使用支付通知方式时,供应商会就公司由于计算错误等而导致支付通知金额小于应付金额的情况与公司电话联系,而如果是支付通知金额大于应付金额的话,自然供应商也很可能放任不管。

此外,一般部门员工如果企图在支付时实施舞弊行为的话(假设他已经回避了供应商主文档中的支付信息等基本控制),核对发票时,有订单、应付账款或其他应付款以及外部发票对其进行牵制。而在支付通知的方式下,不进行与订单数据的核对,只要收款方自身没有异议的话,款项就会被支付,因此,只要能够计入应付账款或其他应付款,支付的舞弊行为就可能发生。

但是，组装型产业中实际使用支付通知这一方式时，我们也可以考虑设置一些相应的条件，比如只限定于支付给有长期供应关系的供应商，并且签订基本合同明确供货品种和价格等。通过这样的条件限制，虚构支付对象、虚构计提应付账款和其他应付款就会很困难，所以不能一概而言这种方式一定会造成什么样的问题。只是至少当限定了一定的状况和交易对象，并且相信支付金额计算处理不会发生差错时，才可以采用支付通知的方式，同时还必须充分考虑其风险。

支付：注意支付流程系统化部分

在讨论支付处理之前，首先让我们来复习一下与支付相关的职责分工。前文提到的20世纪初的例子中，开始出现了会计部长和财务部长的职务分离。在现代，多数情况下会计部长和财务部长不亲自处理业务，且要求支付的记账人员和实际出纳人员必须分离，并希望分属不同部门的不同管理者。

实施支付的人员如果能够同时进行银行余额调整和拥有系统中应付账款记账的权限，可能产生怎样的舞弊行为恐怕已无须说明，实际上，笔者也在不少公司看到过类似的不当事例。让我们在假设满足基本的职责分工的前提下来讨论现代的支付模式。

▼ 企业银行业务系统(Firm Banking System)的控制

以前的支付都是使用票据，而现代的主流是在企业银行业务系统中输入信息，或者系统中生成支付文件，通过磁带、内存、U盘等其他媒介汇总提交给银行进行银行转账支付。但是，我们必须充分认识到，即便是通过这种方式，如果没有同样的控制，舞弊行为还是会发生。

虽然汇票支付方式有所减少，但还是有不少公司在使用。票据的管理一般较好，例如空白票据和未使用支票应在金库妥善保管；空白票据须

连续编号,银行章只能由管理者加盖等,而这些在企业银行业务系统的管理中有时就非常松散了。

企业银行业务系统的软件,通常不是在服务器上而是由财务相关人员的个人电脑进入·此外因为是资金的直接处理,所以大多并没有信息系统部门的参与,因此,很多情况下都没有充分地实施使用计算机时所需要的内部控制。例如,密码长度下限、定期变更、业务必要权限的分配、权限的定期更新等。

实际上在笔者自己看到的多家公司中,有以下一些情况:

- 企业银行业务系统的用户名和密码由多人共有,人员离职时不适时变更;
- 密码只有 4 位,而且还有相同的英文字母或数字;
- 安装有企业银行业务系统的电脑设在办公室出入口附近,而且办公室进入没有门卡的限制;
- 负责确认到账的人员拥有与其业务不相关的付款权限;
- 负责支付的人员在实际操作中可以不经管理者的批准而没有上限地付款。

最后的事例可以在很多公司看到,负责支付的人员如果受到诱惑决定去南美欢度余生的话那就糟糕了。所以说,支票的签字和票据的盖章这样相当于管理者"批准"的行为,在企业银行业务系统也是不可或缺的。

具体而言,可以考虑如下控制:

- 在系统中批准支付·企业银行业务系统内的一个功能是设置只有以管理者用户名登录批准才可以完成支付处理。而且,管理者账户没有输入金额的权限,只有负责支付的员工的账户才可以实施金额的输入。
- 传真确认·将有管理者签字的传真确认件(付款委托书)送交银行,由银行工作人员对企业银行业务系统中输入的金额与传真确认件核对。
- 账户余额限制·(补充控制)在企业银行业务系统中设定账户以

及/或者单笔转账的金额上限。

▼ 生成、送交的支付数据无法篡改

美国 SOX 法案和日本版 SOX 中，针对业务流程和信息系统的内控评价，因为评价者必要技能的不同，而由不同人员负责的情况很多。如前所述，企业银行业务系统往往不由信息系统部门直接管理，所以相关控制活动很容易被从信息系统部门管理的范围中遗漏。相反，从业务流程相关工作人员的角度来看，企业银行业务系统也是“不怎么搞得明白”的系统之一，应该由系统方面的专职人员来负责，或者认为因为是系统处理所以无论如何应该是安全的（当然并不是这样）。

如果是从基础系统中生成磁带或支付文件，“确保应付账款/其他应付款无法篡改”就成了问题的关键。笔者曾看到过这样的例子，生成支付文件后，会在企业银行业务系统中处理，“支付文件只是单纯的文本文件，包括金额都是可以自由改动的”。发生这种情况时，当然就必须与在企业银行业务系统中人工输入时一样，实施先前所举的控制活动。

轮岗和长期休假：内部控制还是植根于文化中的事物

到现在为止本章都在讲述会引起怎样的舞弊行为之类的灰暗的一面，最后想以稍微轻松的话题结尾。

轮岗和长期休假制度作为内部控制最早出现在文献资料上是在 20 世纪 20 年代，是历史上最为古老的内部控制行为之一。

设置轮岗使得人员或部门变更，在长期休假期间由别的人员负责该职务，是旨在发现平时很难发现的舞弊行为的强有力的控制，包括与外部的串通、外部凭证（余额对账单、寄存证明）的篡改等。

但是在美国 SOX 法案或日本版 SOX 中，轮岗和长期休假通常不被认为是必需的内部控制行为（关键控制）。其他控制，例如“批准”是“内容

的检查和斟酌”、“职责分工”是“业务的分担”等，这些都是与提高业务效率目标一致的控制·相反，例如轮岗，可能被认为是违背业务习惯性和专业性的。长期休假多在金融机构实施，在一般的企业并不多见。这一控制在欧洲等有长期休假习惯的国家可能更能被接受。

在中国，轮岗和强制休假制度的实施作为内部控制的一环得到提倡，《企业内部控制应用指引》(征求意见稿)中也记载了希望资金管理、采购、衍生产品的相关负责人员以及销售领域的管理者实施轮岗，资金管理和衍生产品负责人员等实施强制休假制度。

专栏　回扣与经济的文明程度

·内部控制的要点会变化，但是不能没有

有一个世界贪污认知指数调查[1]，根据2007年参与调查的180个国家和地区中，主要的亚洲国家中，以印尼最差，排名143位，菲律宾其次，排名131位；越南排名123位，泰国排名84位，中国排名72位，韩国排名43位，中国台湾地区排名34位，日本排名17位，中国香港排名14位，新加坡排名第4位。

行政努力等要素也起到了正面作用，但客观上来说还是经济发展越成熟的国家和地区，贪污腐败的现象越少。

听说回扣等经济舞弊、贪污过去在中国也屡见不鲜，随着经济的高速发展，近几年情况已经有所改善，但是，根据行业和交易对象的不同，事实上还有很多存在的地方。

在印尼，有常常看到白纸黑字的报道，“政府取缔伪钞部门的制作完美的伪钞”，“海上油田的输油管道装有偷油龙头，以油轮为单位偷油”，“正规海军从事海盗勾当”等。

即使在企业内部，向供应商拿回扣，从在中秋节和盂兰盆节雁过拔毛般地索要礼金，到无限制地虚构订单，发生的频率都相当高。这被称为“礼

尚往来”，互相给予方便，希望得到回报已经成为了习惯，可以说很容易导致回扣的发生（不过好像当地的公司还是认识到，这属于舞弊行为并会导致公司利益遭受损害）。此外，财务负责人超过正常应付金额的不当付款行为也时有发生。

在多数人的印象中，发展中国家内部控制薄弱，而且舞弊情况较多。但是，其实内部控制薄弱和舞弊行为较多实际上是两回事。

根据美国 SOX 法案和日本版 SOX 对在发展中国家的子公司的内部控制实施评价，会意外地发现很多子公司的内部控制设计、运行良好。这可能是因为对于真正危险的环节实施了实质的检查和控制。尽管如此，由于存在同谋、伪造或盗窃等“内部控制局限”的事例，舞弊发生的频率高于平均值。

这里，让我们一起来想一下所谓各国内控评价相关法规所提及的制度化的内部控制是如何与回扣等舞弊问题相关联的（在销售和人事领域的事例当然也有，但首先让我们针对采购和财务考虑）。

（1）发出订单前需要询价，一定金额以上的订单需要取得多家供应商的报价进行比较，并要确保竞价必须有实效。

（2）原则上个别的发出订单，支付批准应由管理层亲自执行。

（3）采购和财务的管理者和从业人员实施轮岗。

（4）检查采购和财务管理者日常生活中有否不同寻常的奢侈行为。

在以上描述内容中，根据美国 SOX 法案和日本版 SOX 实施评价工作时，（2）是会作为控制对象的，（1）和（3）通常很难作为评价内容，但可以考虑添加“采购实施标准”等方法。但是，（4）是个人隐私问题，处理起来可能有点困难。

如前所述，在各国内控评价相关法规的模板式评价工作中，较难发现舞弊方面风险问题的情况很多，但这样的评价自始至终只是表面的文件化和验证工作，必须考虑子公司所处环境和具体情况，实施有实际意义和效果的评价活动。

更不能忘记的是，无论在哪个国家和地区，实际上也正发生着各种各

样舞弊行为，可能就在你的身边。在不同环境中进化的动物，发达的器官也有所不同。同样地，根据环境和文化的不同，要关注的重点会发生变化，但重点本身一定会存在。

注

[1] 名为透明国际(Transparency International，简称“TI”)的国际非政府组织所做的调查。

第七章 存货管理

库存是销售，制造等企业活动的关键节点

实物的安全：为实现资产保全的主要控制

“实物的安全”可以说是最古老的“控制”。请想象一下中国和日本自古以来的悬空式的谷物仓库。将谷物放在抬高的仓库里，可以避免水灾、防止湿气，保持谷物干燥的状态。然而，为了防止盗窃也需要相应的看护。所谓实物的安全，不仅指防止盗窃，防风防水防火的对策、防止变质退化的温度管理等保管状态的适用性也包含在内。

追溯到更远，一般认为“拥有”的概念和实物的安全是表里一致的关系。根据自然人类学的研究，黑猩猩也有“拥有”的感觉，而“手中拿着、随身携带”自然就是拥有的意思。

如今实物的安全是重要的控制。

美国 COSO 内控整体框架报告是目前世界上内部控制架构的标准，其中，内部控制的目标包括了“业务有效性及效率”、“财务报告的可靠性”和“法令等的遵守”这三项。

日本版 SOX 的《实施标准》中定义的内部控制基本架构中，除了 COSO 中定义的“业务有效性及效率”、“财务报告的可靠性”和“法令等的遵

守”三项外，还提出了“资产保全”。虽然看起来像是为了体现日本特色而追加了这第四点，而其实据说是由于在 COSO 制定的过程中，资产保全是作为内部控制目标的候选项，所以并非日本原创。日本版 SOX 的内部控制目标不比 COSO 更宽泛，而是将 COSO 中已经包含在业务的效率和财务报表的可靠性中的内容更明确地反映出来。资产保全与业务的效率以及财务报表的可靠性之间的关系很明确。像这样目标间的重复，在《实施标准》中的“四项目标间的关系”这一部分也进行了说明。

在中国财政部等五部委发布的《企业内部控制基本规范》的第三条中记载，“内部控制的目标是合理保证企业经营管理合法合规，资产安全，财务报告及相关信息真实完整，提高经营效率和效果，促进企业实现发展战略”。与美国 SOX 法案和日本版 SOX 相比，中国加入了“企业实现发展战略”，一共有五项。这据说也是受到了美国 COSO 委员会在 2004 年 9 月发布的企业风险管理整体框架的影响。

毫无疑问，实物的安全是达成资产保全这个目标的主要控制。内部控制架构中主要目标之一的资产保全，不单指存货资产，还包含固定资产、越来越受重视的人力资本、信息资产，甚至是品牌价值。然而，本章的主题是存货资产，即库存，让我们就此进行讨论。

以前，笔者曾和同事有过其他的讨论。比如，“投保保险”是否可以成为实物安全的替代性的控制。

从风险管理的角度来说，存货如果遇到破损、盗窃、火灾、风灾、水灾等时，可以获得保险赔偿，所以可以看作是一种补偿。然而从会计科目的角度来说，存货和（保险）应收款是不同的。确实，即使实物投了保险，我们也不能说就可以放松对实物的保管了。

然而，在自己公司区域内保管的库存当然是按照自己公司的标准来确保库存的安全，而在途物资或者是委托存放的物资，基本上是委托运输公司和委托方来管理。理想的内部控制也许是“对交易方或受托方的管理情况进行调查，如果情况不良的话，就不与其进行交易或委托其保管”。但实际情况是，不管法律或者合约上是否有相关补偿义务，为了确保实物

的安全，公司自己一般还是会对实物进行投保。

这里，笔者认为仓库、受托方或者承运方的补偿条款和保险投保是对存货安全的一种补偿方法，存货资产大部分还是应该满足公司自己的安全标准。预先考虑到这一点就好了。

实地盘点与数量变更的审批：基于“实际是否存在库存”的重要控制

存货管理相关的内部控制历史也很悠久，在第三章采购中曾介绍过20世纪初的原型。

- 仓库管理员（Warehouse，进一步分为负责验收、发货、保管、保全的人员）处理实物。
- 库存管理员（Inventory）管理库存的记录。
- 对应实物的出/入库，仓库管理员负责制作出/入库单，并提交库存管理员。
- 库存管理员将出/入库单的原始凭证在账簿（库存收支分类账）上记录。

是不是觉得与现代普遍使用的流程大相径庭？

与库存相关的内部控制原型在今天几乎都不适用。在欧美企业中，由不同的部门分别负责库存管理和仓库管理的情况很普遍，仓库管理员将仓库/库存管理系统中的原始数据自动传送到会计系统中，最终实物及其记录由不同的两方来管理。那么库存管理员负责哪些业务呢？他们负责那些不应由采购部门操作的价格录入以及运输的安排物流等相关工作。我们作为审计师在考虑内部控制时，通常不强烈要求库存部门和仓库部门的职责分离。

为何现代与20世纪初的原型差异较大，可能原因之一就是通过信息系统的利用，只需由仓库管理员输入一次即可的信息，库存管理员再重新输入的话，很明显地，从成本效益角度看并不合理。

另外一个最大的原因是，存货是能够通过实地盘点来确定数量的。即使实物和记录由不同的人员负责，对于实物被拿走这样的情况，职责分工也是无能为力的，这是实物安全的问题。当实际发生实物盗窃时，通过实地盘点可以发现理论库存情况和实际库存情况的差异。

▼ 存货数量变更时的审批是不可或缺的

内部控制的局限之一是共谋。仓库、库存部门的下属和上司合谋将库存产品运走的情况还算好，最恶劣的情况是会计部门和仓库、库存部门的集体合谋，将理论库存数量修改至符合实际库存数量。这种情况，会在账面上留下不符常理的修改记录。

因此可以说，不仅在实地盘点中要确认存货实物的存在，恰当地实施存货数量修改的审批对于存货的完整也是不可或缺的。

所谓数量的变更，指的是根据实地盘点的结果调整理论库存数量和实际库存数量之间的差异，以及发生报废、废弃，或库存转移。这样的修改一定要在事前得到审批。

反之，根据销售订货的发货、根据采购订单的入库、产成品的入库等之前已经得到审批的行为，其数量的修改不包括在内。库存商品的出入库（特别是搬出）必须伴随有恰当审批的单据，并要求门卫、保安人员对此进行确认是基本常识。对于客户的出库要有出库通知单。报废、废弃货物的搬出，库存转移等，也需要相应的通知单。

此外，回到实地盘点的话题，要确定库存商品是不是真的在那个地方这一事实，销售和采购循环的内部控制同样能够帮上忙。比如，如果产品库存少于账簿数字的话，那么就可能是漏计了销售额（以及应收账款和销售成本）如果多出了材料和零部件的话，那么就可能是和采购相关的会计科目漏计了。反之，如果比账簿数字还多的话，有可能是数据上显示了出库而实际上还未出库，或者客户退货没有计入 如果少了材料和零部件的话，则有可能发生领用或退货给供应商的漏计。

▼ 实地盘点应注意事项

此外，有部分种类的存货可能没有纳入库存记录的管理范围。换句话说，就是没有对这些存货的收发进行记录。例如低值易耗品、促销品、辅料等，往往会在购进（入库）的时点作为费用处理，期末再将剩余实物计入库存的处理方式。如果不进行库存记录管理的话，就不会在期末产生与实际库存的差异 这样的话，就很难发现偷窃或挪用的情形。我们必须充分认识到这样的管理方法（或者说是不管理的方法吧）。我们必须按照公司可以容忍的金额（或者即使发生差错，也不可能会超过财务报告的重要性指标），对该类存货谨慎地予以限定。

此外，我们刚才说到库存实物和记录的职责分离可能在实际业务中已经不太适用，但它却是实地盘点时的注意事项。我们认定有效的实地盘点是库存盘点人员和记录人员两人一组进行。而且，这两个人中的一人必须是日常业务中和库存业务无关的人员。

实地盘点中，其他应注意的事项是对于运输途中以及委托保管的库存等不在自己公司场所保管的存货的盘点，或者使用替代的方法来进行。这样的库存，往往是和销售额的计入有关的。临近期末时进行出库、销售、退货处理以后，往往有以委托保管的方式暂时存放在客户那里这种行为，所以说有必要考虑将其确切地计入存货。

存货的估价 根据明确规定而不是随意地实施估价是很重要的

采取了实物安全相关措施，实施了实地盘点（＋数量修改的审批），那么关于存货数量的相关控制就完美了吗？有什么遗忘了吗？对了，是金额！

我们必须定期对存货资产的价格是否适当进行评估，希望在实施盘点或者日常仓库管理时掌握由于物理损伤而使存货价值减少的情况。与之相应，由于市场原因导致商品期望售价降低的话，也应该在账面上进行

分析。然而，要评估商品的跌价准备是比较困难的。会计的谨慎性原则要求多计提跌价准备，然而不应允许由于过度谨慎而扭曲公司的财务状况和经营业绩的行为。

因此，关于库存产品的老化，一般要根据其滞库时间等数据，客观分析何种情况下应计提多少百分比的跌价准备，这个标准有必要作明文规定。

在中国的会计处理中，容易发生对老化或受损的存货、固定资产不作废弃处理的问题。在美国和日本，库存和固定资产的报废损失在会计上和税务上都能确认为费用，而在中国，为了能作为费用在税前扣除，需要到税务机关实施备案，并根据税务机关的要求，必要时请专业鉴定机关出具证明。但如果作为正常的“销售损失”一般是可以在税前处理的，所以对于一些老化或受损的存货，与其作废弃处理，还不如在可能的前提下降价销售。另一方面，我们也会看到一些公司因为不准备作税前扣除，认为税务上不需要准备任何相关证据，而在报废处理时没有留下任何报废的证据资料。这样的做法在内部控制方面其实是有问题的，因为会计处理也需要相关的凭证支持。

此外，只在系统中做出入库的处理、替换保管期间、表面上缩短呆滞期间等处理是不允许的。

专栏　库存和供应链

• 库存减少的话，现金流就增加了

接下来让我们来讨论一下库存相关的话题，也会涉及一些供应链的相关内容。

如果用一句话表达供应链的目的，可能可以归纳为“（至少狭义上是）减少库存”的活动。这话听起来可能觉得没什么了不起，但是减少库存有各种各样显著的正面效果。

库存的保管费用减少了吗？是的，这是真正直接的费用。

相关管理成本也减少了吗？答对了！实地盘点变得轻松的话，说不定审计师也会感到高兴……可以说，库存本身的费用的减少不过是该效果的一部分。

那么，回答“现金流增加”的人，则具有相当丰富的财务知识。我们来看一下图 7-1，从采购（支付）、制造、销售到收款的流程中，“库存的减少”＝“库存平均滞留期间的减少”，那么投入的原材料和劳务费用就能够尽早回收。粗略地说，“制造需要的时间＋平均库存滞留时间＋应收款回收时间－应付款支付时间”＝“周转资金必要的时间”，其实有必要再加上原材料的库存期间、产品的流通期间等。

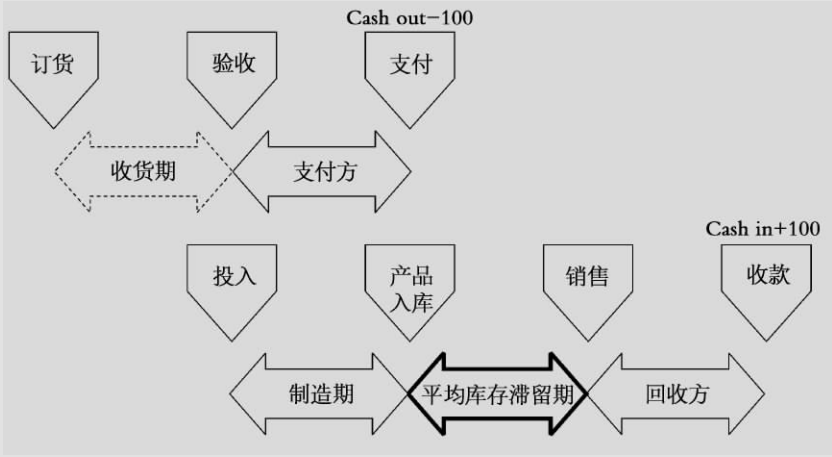

图 7-1　库存和现金流的关系 1

稍微转换下角度，可以认为资产负债表上的存货资产的一部分已经现金化了。见图 7-2。

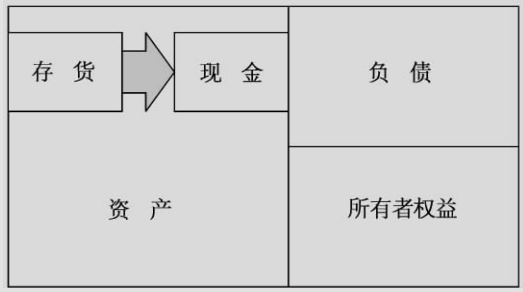

图 7-2　存货和现金流的关系 2

• 新产品推出会明显地导致库存减少

事实上，随着供应链管理的进步，减少库存的最大效果在新产品推出时就发挥作用了。推出新产品的那一刻，现有库存就成了旧产品。如果不等旧产品售完就销售新产品，旧产品就会滞销；或者如果等到旧产品大致售罄新产品再上市的话，新产品实际销售的时间就推迟了。

例如，若能减少平均每月 10 亿元的库存，假设年度销售额有 120 亿元，如果在不等旧产品售完就推出新产品的情况下，就能够达到新产品的发布提早一个月的效果；或者等到旧产品大致售罄新产品再上市的情况下，就能减少滞销库存的损失 10 亿元。因为业界越来越多的新产品的开发让竞争变得越发激烈，能够提前一个月是无价的！

虽然那么说，胡乱减少库存会导致销售机会的丧失。如果是有季节性的产品，于繁忙期前预先积累库存也很必要。为了不丧失销售机会而减少库存，要同时提高需求预测的准确度，在整个供应链上提高信息的传达效率。

因此，正如 PSI（Production-Sales-Inventory＝制造・销售・库存）平衡一词，库存是销售、制造等企业活动的关键节点，同时也是运营方法和战略的成果。

第八章 固定资产管理

资产负债表的重要组成部分！其减值、折旧等会对损益产生很大影响

对于多数企业来说，固定资产很大程度上决定着资产负债表的借方。资产负债表另一边的“负债和所有者权益”主要描述了资金的筹措方式，而企业实际上从事着怎样的经营活动，如何通过在生产、销售和服务环节中有效使用资金来提高竞争力，都反映在资产负债表上“资产”的一边。

然而，“利润表”作为企业的“成绩单”一般更受重视，所以在处理固定资产科目时，说得轻一点是“合法的灵活调整项”，说得重一点则是“可能利用各种财务、会计手段合法地调整入账金额，并体现损失或收益”。就此，近年来会计准则作出了诸多更新，以使“财务报表能够更合理地反映企业的实力”。

美国 SOX 法案规定应根据相关会计科目的金额重要性和风险程度判断固定资产是否作为评价对象，但由于大部分公司会选择八九成的会计科目作为对象，实际上很多企业将其作为评价对象的企业较多。

日本版 SOX 实施标准规定了（在公司层面内部控制、财务决算及报告流程评价之后）要对于“与企业经营目标有重大关联的会计科目相关流程”进行评价。因此，除非是业务在很大程度上依赖于固定资产，多数企业可能不将固定资产科目作为评价对象。但是，实施标准中也提到“关于

重要的业务流程，可以作为评价对象个别追加”，如“固定资产减值损失”等。

在中国，财政部办公厅出台的《企业内部控制应用指引》（征求意见稿）中专门设置了“固定资产”和“无形资产”的章节。

那么，让我们来看一下固定资产方面的通常的管理要点以及所要求的内部控制。

租赁资产：合理地将表外／表内的判断以书面文件形式记录

在日本，由于将固定资产转换为租赁资产会减少固定资产的列报，租赁交易很快得到了普及。与之相比，中国的租赁行业始于20世纪80年代，发达程度远不及美日等发达国家，但2008年来随着需求的增长，固定资产租赁行业得到了迅速的发展。

实际上，无论是向他人借来资金购买固定资产并定期偿还债务，还是租用他人的固定资产并定期支付使用费用，这两者的实物和资金流动很相似。实际操作中，在使用期间、付款金额、租赁合同期满后的买入、合同的更改或解除的罚则、改造、修理、使用年限和残值的估计等方面，要考虑各种各样的合同条款或交易状况；实际上，实物固定资产的购入和租赁交易的界限比较模糊。

然而遗憾的是，在会计处理上只有作为购入固定资产处理的融资租赁（记入贷款和租赁资产科目，作为表内资产）和作为租用固定资产处理的经营租赁（租金记入费用科目，作为表外资产）这两种方式。

在美国，早在1976年就导入了与租赁会计相关的会计准则（1977年1月以后开始适用），详细规定了在何种情况下应以何种方法处理。然而，伴随着金融工程学的发展，越来越多的租赁交易难以辨别是表内还是表外，相应的租赁会计准则也随之进行修改，如此交替的情况不断发生。例如，最低租赁付款额（Minimum Lease Payment）的现值（Present Val-

ue)就是标准之一。笔者听到过这样的案例:使用保证包含最低租赁付款额残值(Residual Value)保险产品的公司,正犯困于为了满足近年来由于租赁相关会计准则的修改而支付越来越多的保险费用。

日本的租赁会计准则中有对于所有权转移以外相关例外的规定,实务操作上绝大多数不记入表内业务。然而,日本准则与国际会计准则融合的潮流正在加快,租赁会计的修改动向也呼之欲出。

而在中国,无论是新会计准则还是旧会计准则,除了土地租赁之外,基本都与国际准则接近。

就内部控制角度而言,无论租赁资产在财务报表表内还是表外,都是企业生产经营活动所必需的设施或设备,必须根据其重要性来进行管理这一点是不变的。因此,必须比照购入固定资产,对取得、处置、转移、实物盘点等实施内部控制。

此外,关于租赁合同本身的管理,在合同内容复杂的情况下(例如,可能有销售方计入销售额,承租方采用经营租赁方式的情况),从会计上的要点来讲,公司必须合理地将表外/表内的判断以书面文件的形式记录下来。介于这样的情况,有时应该借鉴律师、会计师的观点。如果是规范的租赁公司,对于大规模且性质微妙的租赁交易,应该考虑将为顾客寻求法律意见作为工作内容的一部分。

"可见的"固定资产:需要注意处置相关事宜、转移记录、掌握闲置固定资产等方面

首先,让我们来看一下"可见的"固定资产所应该关注的固定资产实物管理要点。

▼ 取得与处置

取得和处置固定资产必须基于适当的批准实施。取得固定资产所需的批准程序一般会包含在采购相关批准规定或投资相关书面协议书上,

而处置固定资产是固定资产特有的程序。正如第七章存货资产中提到的，在中国，固定资产报废处理不能在税前扣除时，经常能够看到公司对报废的证据资料、文件、照片等不予保存的情况。从内部控制的观点来看，希望公司能够保存报废处理的批准和报废的证据资料。此外，应当注意出售固定资产时的程序，例如开发票以及收款的管理会不会有问题 相比产品的销售，在销售固定资产的过程中需要注意不要在程序上草率行事。

▼ 台账管理和转移

已取得的固定资产用固定资产台账进行管理，在实物上贴上与台账对应的号牌或标签。由于租赁资产不是本公司的资产，且将相对价值较低的备件等作为租赁资产的情况很多，所以对于这一块的管理很容易忽视。租赁资产有必要在财务报表附注中披露，同时考虑到向租赁公司的支付管理。台账的使用非常重要。

如今，大多公司已不再使用纸张编制固定资产台账和租赁资产台账，但是因为很多公司不用专业财务会计系统，而使用简易软件或者表格计算，所以有必要注意安全与备份等信息系统整体控制方面有没有问题。

虽然固定资产的转移在会计分录上不作反映，但从管理的角度也必须确切及时地记录。在工作中有没有备件或工具在部门间借用但没有记录的情况呢？因此，有必要在固定资产台账上填写放置的场所，像车辆等移动的固定资产则应该填写主管部门、负责人等，且设定每次发生变更时的程序。

▼ 实物盘点、停用、处置、保存

中国的《企业会计制度》规定了固定资产必须定期或至少每年盘点一次。日本虽在法人税中规定存货的盘点必须每年进行一次，但对于固定资产相关的实物盘点没有明确的法令或者准则加以规定。有部分公司能够实现每年对固定资产实施实物盘点，但还是存在为数众多的公司多年

未对固定资产进行盘点情况。

根据实物调查，对于已认定为不能运转的固定资产必须将其分类为闲置资产。尤其在资产减值会计处理被引入后，由于闲置资产的会计处理发生了变化，故一定要实施必要的控制。困难的是，模具等用途有限的固定资产，今后是否会使用，还是会被报废尚且未知，在某些情况下必须向产品的供货方确认后才能作出判断。

我们在第七章中提到过，中国的《企业内部控制基本规范》和日本SOX的《实施标准》将“资产保全”都作为内部控制的目的之一。通常情况下，固定资产的转移较存货困难，然而，有必要防止发生未经批准的固定资产搬出、转移等。此外，在固定资产的资产保全方面还有一个重要特征，那就是必须注意与生产设备相关的劳动安全事项、与建筑物相关的法规、消防法等众多合规关联事项。

“不可见的”固定资产：采用资本化还是费用化会导致损益的很大变化

一说到“不可见的”固定资产也许就会想象是无形资产，而这里更加宽泛，应该资本化的修理费用和固定资产折旧等与无形资产一并在这里讲述。

▼ 修理费用和固定资产折旧

符合资本支出的修理费用要计入固定资产，不过实际操作部门经常会将这一点遗漏，而仅作为费用通知会计部门。

此外，记账时，以怎样的归纳方式在台账上记录也相当重要。部分更换、部分报废的时候，需要弄清楚各个部分，然后分别确切登记。发生部分毁损或停止使用的情况时也是如此。

对于固定资产折旧，虽然税法中已详细规定了何种资产以何种使用年限计提折旧，但有时税务的标准不一定适用。虽然在中国和日本这样

的做法不是很普及，但在欧美，很多情况下公司会区分管理会计上的折旧和税务上的折旧。如果税法的标准和经济实际情况发生很大的背离，那么会计上和税务上的折旧就应当分开管理。这一点其实也适用于将修理费用作为资本化支出的部分。

同时，固定资产的使用年限直接影响计提的折旧费用，从而会对损益产生很大的影响。如果实际使用的固定资产的估计使用年限因故发生变更时，需要将其作为“会计估计变更”，和会计政策变更一样需要得到批准。

▼ 研发、软件

在中国，尽管研发和信息系统软件通常价格较高，但实务上常有未得到正确处理的情况，比如将研究阶段发生的费用或无法满足无形资产的定义及相关确认条件的开发费用作资本化处理，或将应计入资产的软件作为费用来处理，或者不管其性质统统计入资产等等。从内部控制的角度，公司需要按照适用会计准则的规定实施相应的会计处理，并将会计处理的依据以书面的形式记录下来。

▼ 知识产权

知识产权是一种无形财产权，是从事智力创造性活动取得成果后依法享有的权利。中国新会计准则中，专利权、非专利技术、商标权、著作权、特许权等都属于无形资产。商誉的存在无法与企业自身分离，不具有可辨认性，所以不属于无形资产。

在日本，商誉在企业收购时被计入在相关账户中，不过根据适用于2005年4月1日以后开始的会计年度的减值会计，如果目标企业由多个业务单位组成，那么原则上将每个业务单位的商誉分开记录。据此，收购的目的是获得特定的市场和大型贸易伙伴，如果获得（不作为商标权计入的）品牌，那么可以说也应该将其分开记录。和刚才提到的作为资本支出的修理费用类似，该特定的业务、市场和与大型贸易伙伴的关系、品牌价

值发生毁损时，需要计提各种各样的减值准备。

关于特许权和商标权等的知识产权，我们在这里先不谈大家比较感兴趣的取得时估价的妥当性，从内部控制的角度看，关键是每期都有必要合理确认是否有减值的迹象。当然，有形固定资产也是一样，但是有形固定资产相对比较容易判断其实物是否可用、是否损毁，且使用台账进行管理一般不易遗漏，而无形资产是否报废等判断的难度则相对较高。此外，美国准则要求对无法确定使用年限的无形资产不进行摊销，而是至少每年对其进行一次减值测试。

在中国，企业取得的土地使用权通常应确认为无形资产，但改变土地用途，用于赚取租金或资本增值的，应当将其转为投资性房地产。这与其他国家有所不同。

减值会计的含义：旨在使资产负债表能够更好地反映事实

中国的旧会计准则中已经引入了资产减值会计的思想。为进一步规范资产减值的确认、计量和相关信息的披露，新会计准则增加了《企业会计准则第 8 号——资产减值》，明确了资产可收回金额的计量方法，使资产减值损失的确定具有较好的可操作性。此外，新会计制度在会计核算方面有很大改变。旧准则规定已经计提减值损失的资产，如果资产价值恢复，则资产减值损失可以转回；但根据新准则，大多数资产减值损失一经确认，在以后会计期间不得转回。这将有效地遏止上市公司利用减值准备调节利润。

减值会计的导入，是以“在资产负债表上反映更实际的情况”为首要目标的。不过更值得关注的是，将“运用该资产从事经营活动从而产生的损益和现金流”作为判断的基准之一。这意味着，在会计准则中包括了“应该根据固定资产在经营中产生的现金流来评价该固定资产的价值”的考虑方法。

1990 年前后，日本发生地产泡沫。究其原因，主要是无视现金流，在土地预期价格不断上涨之下购买不动产的逻辑在一流企业中盛行，同时银行、非银行金融机构也无节制地对这些企业融资，最终导致大量资金流向土地和建筑物。之前也提到过，由于趋于轻视盈利是日本企业很大的特点，日本的经济和社会的某些方面（间接金融、终生雇佣等）也是在此基础上形成的。可以说减值会计的诞生是日本企业向美国型企业转型，在经济方面变化潮流的一个环节。

随着中国经济的发展，土地使用权、房屋建筑物等日益成为企业和个人投资的对象，致使价格出现过度高涨的倾向。企业对于不动产的认识和运作也逐渐开始适应国际化的进程，开始运用租赁和资产支持证券等方法。

只是，任何事做过头了就会滋生弊病。从所谓的总资产回报率（ROA）和净资产回报率（ROE）等财务指标的观点出发，可以说是资产越少越好。极端地说，完全不持有固定资产而只进行投资，比如对冲基金那样的企业也许有着最好的商业模式。

企业所处的行业在很大程度上决定了“哪些资产、设备作为固定资产是必要的？”这类问题。损益表里的主营业务利润、资产负债表里的资本充足比率等还能勉强用于跨行业的企业比较，但如果要回答固定资产处于何种状态最佳，那么，如果不联系该行业实际的话就很难说了。

在会计准则中表现出的重视利益的潮流，鼓励了企业在短期内收回投资 换言之，在适应第三次产业高速发展的同时，可能会冷落了需要长远投资眼光的大规模重型工业产业。

第九章 资 金 管 理

与资金有关的舞弊将动摇企业的根基

金融衍生产品管理：企业需要的是明确的、具有可操作性的政策

与资金有关的交易产品中，一般认为风险最大的应该是金融衍生工具。实际上，“衍生工具”这个词本身就会给人感觉是偏离实业的金融机构的产品。但是，衍生工具原本是一方支付一定的手续费从而降低风险的需求、另一方收取手续费以承担风险的交易。如同保险一样，这是自然产生的产品。

实际上，世界上最初使用现代衍生产品的是日本江户时代 1730 年开设的位于大阪堂岛米会所的期货产品。诸藩有实际需求，希望确定预备生产的大米价格，并将一部分变卖。米商接受未来商品价格，并可以对权利凭证本身进行交易以赚取净利润。

让我们再追溯而上，如果列举人类最伟大的 30 项发明，货币一定会名列其中。世界各地根据实际需要，自然而然地产生了各种材质、各种形状的货币。随着产业的发展和经济活动的复杂化，交易方式当然也越来越进步。

但是工具和技术若使用错误，将带来危险。比如火和刀都是非常便

利的人类发明，但是同时要注意不能让人被烧伤或者刺伤。同样道理，在使用衍生产品的时候也要建立适当的风险管理手段（内部控制）。

关于衍生工具的内部控制，首先要注意建立使用衍生工具的明确制度。到底仅是根据实际需要（风险对冲）来使用衍生工具，还是出于追逐利益的原因使用衍生工具（投机）？一般来说，除了业务本身就承担投资风险的金融机构和投资基金，其他的企业应该在公司内部规章中说明衍生工具必须仅为风险对冲而使用，并进一步限定使用种类。例如，仅限于汇率远期、利率掉期等具体的工具。

即使是根据实际风险对冲需要使用衍生工具，管理层的审批仍然必不可少。如果与投机活动相关，企业必须根据实际承担风险的程度建立相应的审批手续和规则。

▼ 可以参考套期会计的原则来判断使用衍生工具的目的

然而，人们往往难以判断是不是真的根据实际风险对冲需要使用衍生工具。比如，企业预测到会有以外币计价的订单，于是不得不进行相应的采购和生产活动，为了锁定利润额，自然会尽早约定远期汇率。但是，理论上说，在订单还没有确定的情况下就约定汇率，相当于将全部利润暴露于汇率风险下。

套期会计相关的会计准则可以成为一个判断标准。因为企业可以考虑不同的衍生工具是否适用套期会计，它们在财务报表及附注中有不同的披露要求。但是，套期会计相关的会计准则在美国、日本和中国（套期会计和国际财务报告准则非常相近）这三国之间目前来说有很大的不同。

对于已经使用的衍生工具，企业必须建立良好的台账管理，记录合同的条件、金额、风险说明及衍生工具的对方。

而且，尤其重要的是，企业须确认衍生工具合同实际上和交易对手互相核对。具体举例来说，应由和衍生交易无关的独立的其他交易人员从交易对手处获取计算表，并与公司内部的衍生工具台账相对照。

中国航油(新加坡)股份有限公司(简称中航油)是一个典型的衍生工具投机失败案例。经国家有关部门批准,中航油自2003年开始做油品套期保值业务。但管理层擅自扩大业务范围,从事石油衍生品期权交易,但一直未向中国航油集团公司报告,中国航油集团公司也没有发现。该期权交易致使中航油在清算时造成账面实际损失和潜在损失总计约5.54亿美元。2005年6月3日,外部会计师发布了有关中航油巨额亏损的最终调查报告。报告认为若干因素单独或共同造成了公司在期权投机交易上受到损失,包括没有按照行业标准对期权仓位进行估值,没有正确地在公司的财务报表上记录期权组合的价值,缺乏针对期权交易的适当的及严格的风险管理规定,公司管理层有意违反本应该遵守的风险管理规定等。

另一个典型案例是中国国储局2005年的铜期货巨额亏损事件。中国国储局一名交易员在LME(伦敦金属交易所)铜期货市场上通过伦敦金属交易所场内会员SEMPRA,在每吨3 000多美元的价位附近抛空,建立空头头寸约15万至20万吨。铜价格的一路上涨给国储局带来巨额损失。在国储铜事件上,交易行为由原来的两个岗位变成由该交易员一个人操控,背离了内部控制职务分离的原则。

衍生工具的市值确认非常重要。企业须对衍生工具的财务特点充分了解和评价,并由管理层建立相应的制度。

在中国,似乎使用金融衍生工具的企业为数尚少。但是,听说还是有些公司使用了衍生工具,以此减轻了原材料价格高涨对经营的影响,并实现了比同行业平均更高的利润。如开头所述,企业通过成熟地使用衍生工具,可以降低风险。企业须以构筑完善的管理体制为前提,积极地审视衍生工具的管理。

投资、借出资金的管理:企业应以发展主营业务为重

无论是投资还是借出资金,企业都须根据金额和风险程度确定相应的管理层审批权限。而且和衍生工具相似,投资和借出资金也必须实施台账管理并定期通过市值评估。

由于投资和借出资金记为资产,所以内部控制方面必须确认其真实存在性。资产的确认必须由不负责该资产管理的其他人员实施,这一点尤为重要。

上市公司浙大海纳 2003 年年报、2004 年半年报披露的银行存款都有两亿多元,但在这期间,大股东及关联方多次私自从公司账户上划走巨额存款,实际银行存款不到一半。另外,大股东不仅喜欢现金,还喜欢国债。截至 2004 年半年报,披露的债券投资额实际上全部落入了关联方的囊中,公司的国债账户空空如也。大股东有此"胃口",上市公司也在行动上予以配合。

而且,投资或借出资金对象无论是谁,都不像衍生工具那样简单的是一个承担风险或是降低风险的问题。这关系到留存资金的运用、采购方和销售方的支持、和同行业企业的合作、对子公司和关联方的出资等考虑,和本业相关的各种战略目标都相联系,并不是单纯地承担风险。

近年来,面向消费者生产商品的制造业也开始顺利地开展金融业务。通用电气(General Electric)、通用汽车(General Motors)的财务公司特别有名。它们从方便消费者购买自己公司产品的金融贷款起步,通过赊销收取利息,帮助了主营业务的发展。

面向消费者的金融,其本身有很高的利润率。但是如通用汽车,主营业务虽然不景气,但是财务公司业绩很好,这恐怕只是数字的游戏。在美国,相关的融资和信用卡使用已经非常普遍。在这样的地方,制造商的价格战略中,首先考虑降低利率,其次才是商品本身的降价。通用汽车的

“零利率”策略在报纸中也有报道，这样低的利率只是为促进消费者购买产品而已。

在会计处理上，对于财务公司来说，因为利息收入是“营业收入”，财务公司根据消费者的信用状况将正常的利息记为营业收入，而与实际利息的差异部分由汽车公司通过销售费用对财务公司予以填补。在财务报表的分部报告中，看起来好像主营业务不景气但是财务公司业绩很好，实际上利息的减免是产品打折促销的一种手段，我们应该将主营业务和财务公司业务合并起来分析财务报表。

借入资金的管理 还款到期日检查和资金周转

借入资金有多种形式，除了简单地从金融机构借入资金外，还有公司债券、可转换公司债券以及资产支持证券等形式。资产支持证券是以资产为担保借入资金的形式。它不仅是资金周转的问题，而是以应收账款为资产对象，在财务报表上多表现为出售应收账款以回笼资金。资产支持证券在中国 2006 年 5 月 16 日中国证监会发布的《关于证券投资基金投资资产支持证券有关事项的通知》中已经提及，但是实际使用的很少。

借入资金的内部控制，从基本要素上说，也是和存在性相关的审批、台账管理以及和交易对手的复核（具体来说，从贷款人处获得计算表并和台账相对照）。如果从借入资金本身的特点来看，到期还款日检查和相应的资金周转管理显得非常必要。

对于附有财务限制条款（Covenant Clause，比如合同规定，股本比率、分红情况等财务数值须确保在一定数值以上或者以下）的借入资金，为了遵守财务限制条款，企业必须有定期的复核。公司债券发行附条款的情况往往比较多。即使是从金融机构借入的资金，在金额巨大或者内容复杂的情况下，例如，针对公司所有的应收账款进行资产支持证券化时，金融机构有时候会要求公司维持某些财务指标在一定值以上。

▼ 财务相关的三个方面的审查要点

表 9-1 总结了财务相关的主要三个方面的内部控制审查要点。

表 9-1　和企业相关的环境要素相互关系示意

	审　批	台账管理	定期复核			
			市值评估	对交易对手的确认	资金周转	财务限制条款
衍生工具	0	0	0	0		
投资、借出资金	0	0	0	0		
借入资金	0	0		0	0	0

关于台账管理，第八章‘看得见的固定资产’中的‘台账管理与移动’项目中写道，固定资产的台账往往通过简易的软件或者表格计算管理，必须关注安全和备份等信息系统整体控制。同样，这也适用于衍生工具、投资、借出资金和借入资金的台账管理。特别是借入资金的还款和衍生工具的履行，若操作上有差错，将带来严重的后果。

关于借出资金和借入资金，包括现金管理、现金流量系统控制在内的全面管理可能是最佳实践。对于衍生工具，虽然系统并不适于管理特殊和复杂的事物，但是根据实际需要不得不采用衍生工具交易的情况下，由于汇率远期约定等已是定型的工具，根据交易规模和数量，还是由系统管理比较合适。

由于公司债券记入负债类会计科目，企业需要实施借入资金相关的内部控制。除此之外，由于公司债券属于公开发行的有价证券，对于其发行、偿还需要实施和股票相同的管理。至于可转换公司债，需要做潜在性稀释股票(Dilutive Security)计算，其商业上的性质和管理上渐渐接近于股票。

出资方作为‘股东’影响公司的经营是理所当然的；然而，如前所述，如借款金额巨大，那么公司的经营状况和借出资金者也会存在重大的利害关系。很早之前，财务报表的最初目的就是为债权人提供财务信息。

所有者权益的管理：今后的课题是，怎样的“内部控制”适合企业

所有者权益从本质上来说，不会发生经常性的交易。至今为止，还很少有人考虑所有者权益需要怎样的内部控制。可以想到的内部控制包括（包括股本变化的）资本明细的定期复核、与登记簿和从证券代理机构（信托银行）获得的股东名单相互对照。

股票的发行、减资等与公司法、证券法等多个法规制度相关。为了准备好董事会决议、对股东和债权人的通知、登记等合规性要件，企业必须准备一份检查用的一览表（可以从证券代理机构等处获得），在股本变化的实施过程中使用。同样道理，公司债券、可转换公司债券也以此为准。

中国的上市公司屡次出现虚假出资、挪用资金等事件。比如20世纪90年代曾被称为“中国股市第一案”的“红光案”，红光实业涉嫌虚假出资，编造虚假利润，骗取上市资格；沙报亏损，欺骗投资者；隐瞒重大事项，挪用募集资金违规买卖股票，未履行重大事项的披露义务。骗取配股资金也是上市公司的重大舞弊手段之一。比如山东巨力公司原董事长和原财务处副处长涉嫌虚增1999年度利润16 145.73万元，骗取了配股资格，于2001年在深交所配售发行股票1 149万股，共募集资金15 971.1万元。公司成功配股之后，多项配股募资项目却发生变更。相关负责人由于涉嫌欺诈发行股票亦被追究刑事责任。

也许人们认为内部控制（尤其是在传统的业务流程层面的内部控制上）难以防止上述舞弊事件的发生。然而，今天的内部控制登上历史舞台的契机是，安然和世界通讯通过虚假报告以哄抬股价的舞弊事件。由此，2002年美国制定了企业改革法——萨班斯（SOX）法案。

▼ 尝试对“股份公司”体制作出新调整

中国于1990年成立了上海证券交易所和深圳证券交易所，普通市民

可以通过交易所进行证券交易。证券交易所的成立为中国经济发展奠定了良好的基础。

实际上,“股份公司”和“货币”一样,被称为人类的伟大发明之一。股票市场是一个中介场所,连接了拥有生意和业务但是没有资金的人,以及虽然有资金但是不能有效使用的人。它使得社会整体资金利用的有效性取得了飞跃性的提高。股份公司这种组织方式的广泛采用,也支持了产业革命。

人们从早期开始就对“资本主义”的各种缺点提出批判。自由竞争的结果,是胜者垄断或者成为寡头,从而变得缺乏效率。

所有的体制都需要管理维护和调整。在现代经济中,股份公司高度发展和日趋复杂。“内部控制”的明确义务也许是股份公司尝试的调整之一,包括美国 SOX 法案、日本版 SOX,还有中国的《企业内部控制基本规范》及其指引的征求意见稿等都是对其的最新锐尝试。

第十章　财务决算(1)：单体决算

与财务报告相关内部控制中最重要的业务流程

决算流程的重要性：美国 SOX 法案的重大缺陷大多数与财务决算相关

终于说到会计部门的专业领域——决算流程——的内部控制了。

财务决算和报告流程是最重要的业务流程。其原因当然是，美国 SOX 法案、日本版 SOX 以及中国内部控制法规（“中国版 SOX”）的目的均是确保财务报告的可信度。

但是，和前面第九章资金管理中“所有者权益的管理”相类似，财务决算方面的内部控制从前（美国 SOX 法案之前）很少被大家商讨。因为不管怎么说，外部审计师都要对财务决算流程结果制作出的财务报表等是否准确进行审计，所以从前对于制作财务报表的过程认为是不需要研究的问题。正如第四章“内部控制的原点”中所述，以往内部控制是审计师仅为了更有效率地进行报表审计时才会评价的对象。比如在销售循环中，如能确认销售收入和应收账款的记账流程是良好的话，据此可以减少检验期末应收账款余额和年度销售收入的必要的样本量。但另一方面，由于财务决算过程中的重要分录众多，从实施报表余额审计的观点来看，与其泛泛而谈流程，还不如审查每一笔分录更加干脆。

然而,已经生效的美国 SOX 法案、日本版 SOX,以及即将生效的中国版 SOX 中,要求公司设置能够恰当地进行财务决算的流程、人员和内部控制。换而言之,就是对"财务报表的制作是经营者的责任,外部审计人员对于其正确性、合理性进行独立的鉴证"的职责分工进行再次确认。

在中、美、日各国的内部控制法规中均提及,如内部控制存在"重大缺陷"[1],则必须在内部控制报告中进行记录并向公众披露。实际上,被报告最多的问题是围绕财务决算流程的缺陷,这固然是因为财务决算流程是对金额有重大影响的业务流程,但是估计更大的原因是这个流程中的相关内部控制从前没有被大家重视。

▼ 原因是"流程的缺陷"和"人员不足"

接下来,我们来看看美国 SOX 法案如何来披露"重大缺陷"。

虽然第二年以后的结果也出来了,我们这里还是关注第一年的结果。在初次应对 SOX 的 2004 年 11 月 15 日至 2005 年 11 月 14 日中,3 701家公司提交了内部控制报告书,591 家公司(15.9%)披露了一个以上的重大缺陷。

图 10-1 的"合并决算"及图 10-2 的"以前年度调整"、"决算调整事项"是明显与财务决算流程相关的内容,这些实际上在财务报表审计中发现的会计处理、披露错误,被外部审计师批评为"流程缺陷的原因",成为不得不进行报告的内部控制缺陷。

稍微解释一下其他的问题点。图 10-1 的"收入确认"既是关于销售流程的问题,但从"会计方针的选择和适用"观点来看,又是财务决算流程的问题。此外"税金相关的资产、负债"的主要问题是递延税金资产(转回的可能性、估价的妥当性)及应交所得税(预提金额的妥当性)。对于前者,必须判断企业未来预期是否有的应纳税所得额。这点既是税务流程,又是财务决算流程。

日本嘉娜宝事件中,公司大约多计了 2 180 亿日元的所有者权益,为

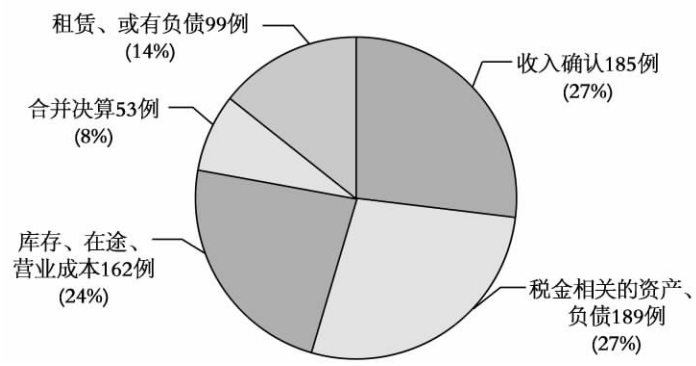

图 10-1　美国 SOX 法案实施第一年披露的重大缺陷:会计处理观点出发的重大缺陷

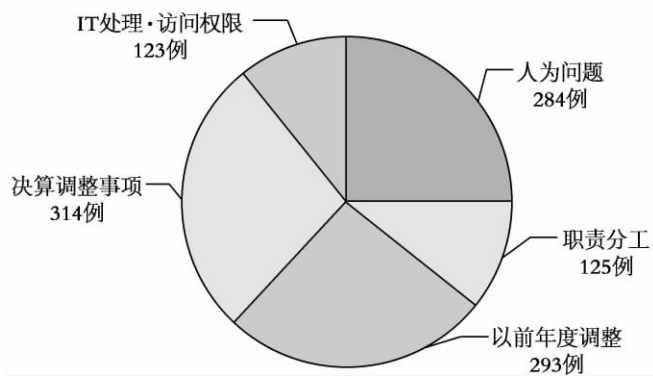

图 10-2　美国 SOX 法案实施第一年披露的重大缺陷:内部控制观点出发的重大缺陷

资料来源:AuditAnalytics. com-May2, 2006 Section404 ICMW Dashboard Year 1 & Year 2.

日本经济史上最大的报表粉饰事件。在 9 年间,嘉娜宝公司通过虚构收入、递延销售费用和管理费用、不将子公司纳入合并范围等积累,在 2003 年 3 月决算时被发现报表存在粉饰,调整了大约 360 亿日元的高估利润,其中 270 亿日元是由于不正确计入递延税金资产而造成的。

判断内部控制是否存在‘重大缺陷’的最首要的标准是对财务报告的影响金额。正如上图所示,公司应当特别关注内部控制中财务报告风险最高的领域,也就是以错误和肆意的操作导致对金额产生重大影响的财务决算和报告流程。

图 10-2 的“人为问题”,具体来说有两类。一种是未按照财务决算要求进行复核、对比等问题,这属于会计部门人员不足(量的问题);另一种是由于缺乏能掌握会计准则的人员,而未能采用恰当的会计准则的问题(质的问题)。大家多用“人为”问题进行委婉的表达。

现在的财务决算流程中,“遇到难以确定的会计处理时,和会计师一边商量一边进行财务决算”的公司可能比较多。这样的话,审计报酬不仅是为审计发生的费用,还包含了支持财务决算的业务委托的性质。此外,审计师审计对象时可能包含自己的判断,从独立性的观点来看也会产生问题。

▼ 积极设计内部控制的企业,其资本成本较低

据说,采用美国 SOX 法案的初期,为了对应法规而展开内部控制的评价和强化的费用,以及外部审计师进行内部控制审计而发生的审计报酬的增加,成为了企业的过度负担。在日本,经过相关部门努力,将应对日本版 SOX 时企业的负担控制在合理范围内,但是发生相应的费用还是不可避免的。在中国,中国版 SOX 采用后的费用尚属悬念。

因为美国 SOX 法案、日本版 SOX 和中国版 SOX 基本上都是对于上市企业的要求,这些内部控制相关的新制度的费用,用一句话来说就是“上市费用的上升”。

简单回想一下,美国的安然、世通以及日本的嘉娜宝、活力门等的粉饰报表事件,成为了这种制度的起因和推动力。通过此,我们就可以得出下面的结构:

报表粉饰事件→上市费用上升

就像特定的企业尽管支付了保险费,但是由于事故、火灾等,造成以后的保险费上升。这种结构很相似。

事故、火灾→ 保险费用上升

为了避免这种负担,有少数的企业放弃了在证券交易所上市,实在是

可惜。无论如何，股票市场是支撑市场经济的最重要的公共设施，我们不得不支付维持其健全性的费用。并且，披露内部控制的重要缺陷对于公司股价和公司地位当然有影响，但据调查结果表明，积极设置内部控制的企业，其资本成本较低。

财务决算流程要求的主要内部控制：外部审计师要彻底“外部”，不能成为内部控制的一部分

接下来，我们一起来看看财务决算流程中主要的内部控制。

▼ 财务决算流程的定义

公司需要用可见的形式来定义公司的财务决算和报告流程，并且可以具体制作成以下的文件：

- 《决算处理指南》：财务决算的处理倾向于依赖个人，容易变成“只有某某可以做”，所以对于主要的处理，需要书面规定其程序和规则，其中包含了确保可交接性等有关业务效率的规定。公司应该不仅只制作单个会计事项的处理程序书，最好将其归结成财务决算处理的指南集。并且，该指南不仅在初次发行时须经过批准，内容变更时也要记录下变更的内容并且再次被批准。
- 会计部门内的《职责分工表》和担当者的《岗位说明书》：特别从职责分工的观点来看，最好能定义财务决算分录的制作人和审核人。
- 《财务决算日程表》：该表明确财务决算在何时从哪个部门获取何种信息，然后在会计部门内处理，最后何时提交给董事会等。公司最好能列举相关的步骤，设定期限、担当者，并且向各关联部门提交文书。

▼ 会计准则的理解

为正确进行财务决算，需要确保有熟知公认会计准则的人才，并且有

必要设立理解会计准则变更的流程。

在这里,如何定义外部审计师的职责往往就成为一个问题。“会计师复核公司的处理是否按照会计准则进行”的情况下,外部审计师代替了公司来实行内部控制。外部审计师要彻底“外部”,不能成为内部控制的一部分。

可行的做法是“财务决算责任人、担当者应当和会计师定期会话,书面接受最新的会计准则信息。在财务决算处理中,对于会计准则有疑问的情况下,适时商谈获得回答。”也就是说,公司事先就会计事项适时咨询外部专家,寻求帮助的话就没有问题(但是,另一方面的难题是,审计师事务所可以在多大程度上提供帮助)。

再有,“事先、适时商谈”很重要。在财务决算开展后,作为审计的一环,让外部审计师看是否恰当运用会计准则,如果发现差错,公司没有能恰当运用会计准则,这些就会成为内部控制缺陷。所以公司一定要进行把握和判断能事前商量的事项的最低限度。比如,考虑准备企业会计准则操作指南、定期购买阅读专业会计杂志、参加外部讲座等。

此外,在美国,审计师事务所往往会提供数百页的最新的 GAAP 的核对表,让企业作为内部控制的一部分进行自查。在日本,为应对日本版 SOX,各审计师事务所正在研究制作类似的会计准则核对表,更新并提供给客户。

▼ 会计方针的选择和适用

正如“财务报告不仅是记录过去发生的事项,也是基于会计方针合理估计的汇总”所述,会计方针的选择和适用极大地左右着报表。因为按照一贯性原则,没有合理的理由就不能肆意变更,也不能随意选择对己方有利的解释。并且,在会计方针的选择和变更情况下,需要用文件记录其依据及相应的批准。

并且,不仅财务报表附注中所记载的重要会计方针需要批准记录,具体的会计处理的内容也应作为批准对象。比如说,销售收入在出库时确

认，由于以不同的凭证作为出库的根据，会造成微小的差异。此外，公司也应当对固定资产的可使用年限、坏账准备比率的计算方法、长期滞库存货的减值准备等，进行明文规定并且获得批准。

此外，会计方针的变更是基于下文谈及的“重要的预提和判断”，最好经过公司内部的独立机构，如审计委员会的复核。由于对象大小不一，不仅应当要报告、审批“重大会计方针的变更”，还要报告、审批那些对于业绩影响较大的会计方针、估计、处理的采用或者变更。正如上例所述，由于会计处理变更造成销售收入、利润等的重大变动也需要报告。

▼ 信息收集

为了使财务决算可以适时正确地收集必要的信息，就需要设计相应的手续和信息系统。从各部门收集的信息纷繁，可以考虑将情况大致分为每日处理的会计原始数据，以及每月、每季度或者每半年处理的会计原始数据两种。

美国 SOX 法案和日本版 SOX 要求公司具备期末决算相关的内部控制，然而，活用信息系统，并且尽可能多地实时记录每日信息，便可对快速正确的财务决算做出贡献。例如，如果库存准确度较高的话，公司可以采用循环盘点，且在结账时就不需要停止出入库。但是，即使在高度信息系统化的条件下，我们也需要考虑到还有一些必须定期手工收集的信息，不应勉强为了尽早结账而不处理那些晚于报告截止日的信息。

很多大企业根据“重要性原则”，倾向于马虎地应付一些细微的会计处理。由于数字有累积效应，故我们要形成正确地对待每一笔分录处理的文化，如有必要就不惜设计相应的体制。这种积极的态度，同样反映在公司业务和事业战略的精心行动中。

▼ 经常性／非经常性交易的定义和批准

经常性／非经常性交易的定义和批准是我们在财务决算和报告流程相关内部控制的文件记录及评价中一直遇到的问题。笔者工作的审计师

事务所的模板中有“关于非经常性的事项、交易的区分的定义”之类的问题,但是这样定义的企业几乎没有。然而,在美国 SOX 法案的审计准则(AS2)中有如下作为让大家关注会计处理的代表性例子:“非经常性(non-routine)交易”是“审计师必须掌握和评价的公司处理流程之一”。

于是,在实务中(笔者自身),由于“非经常性”本来就很难定义,将其解释为“未定义的事情就是非经常性”。所以,具体来说,前述的《财务决算处理指南》中记载的处理是“经常性的”,未记载的就是“非经常性的”。

此外,我们要求在总账中直接输入的分录的制作人和相应的批准人应该分离,对于“非经常性”交易,更需要管理财务决算的高层责任人进行批准。

例如,公司设计用于非经常性、异常、特别处理的凭证,也可以用于前述的选择、变更会计方针和会计处理,并且获得管理层的批准。并且,和财务决算处理指南规定内容相悖的处理情况也是“非经常性的”。

但是,对于会计部门较小的情况,制作《财务决算处理指南》已经很困难,而且在实务中也不太需要。这种场合,只能全部叫做非经常性。由于决算分录较少,所以财务部长或者总经理复核所有的决算分录便可应对该情况。

尽管如此,企业需要准备与其规模相应的《财务决算处理指南》。第十一章合并决算中也会涉及这块内容,我们强烈希望大型上市企业应对其国内外的子公司分发《集团财务会计方针》、《会计处理指南》,并要求其遵守。

▼ 独立机构的复核

对于重要的估计和重要的判断,需要向独立机构进行报告,并接受其复核。

“重要的估计和重要的判断”中,除了在开头列举的递延税金资产、应付所得税等的估计外,还有需个别进行的坏账准备金的判断,规定外的库存减值、损失相关的判断,合并决算的对象子公司的判断,以及会计方针、处理的选择判断等。

美国的公司一般会设立审计委员会或内部审计部门，作为独立的机构。

在日本，公司法规定了一种“委员会设置公司”，即承认公司采用美式的公司治理，但是采用该治理的公司却极少。内部审计部门，好的情况下向社长（而不是向董事会）报告，更多的情况则是成为财务关联部门的一部分，这样就会造成对财务决算责任人和其下属的部门没有独立性。日本公司中有“监查役”（与中国公司的“监事会”相似），然而这一功能如何强化，以及如何才能实施有效监督已成为当今的重要课题。因此，要求“独立机构的复核”在实务上就变得较为困难。然而，切实实施独立复核，可以有效地防止管理层粉饰报表。

在中国，设立各种委员会的上市公司较多，也有设置审计委员会的。但是，美国的审计委员会是作为董事会的专业委员会之一而存在，独立性较高。与之相对，中国的审计委员会独立性比较弱。《公司法》第四节第一百一十八条要求股份有限公司设立监事会，并要求其承担对经营实施监控的责任。然而和日本的监查役一样，如何实施有效监督也是当今的重大课题之一。

以上我们看了关于财务决算内部控制的概要，正所谓“财务报告不仅是记录过去发生的事项，也是基于会计方针合理估计的汇总”。在各国法规出台之前，财务决算和报告流程可能会被某些人理解为，不仅是制作财务报表，还包括了人为“调整”财务报告的可能性。但是美国 SOX 法案、日本版 SOX，以及中国版 SOX 中最重要的要求是上市企业在财务决算和报告流程中排除肆意的操作，通过披露其原本面貌，提高资本市场的透明度，保护投资者。考虑费用和效果的平衡，认真应对该要求是上市公司不可逃避的责任。

注

[1] 根据美国 SOX 法案的定义，重大缺陷（Material Weakness）是最为

严重的缺陷。美国 SOX 法案中,内部控制的问题点定义为“重大缺陷”、“重要缺陷”及“缺陷”三类。

日本版 SOX 中定义为“重要的缺陷”和“缺陷”两类,看起来略有些微妙差别,但美国 SOX 法案的“重大缺陷”和日本版 SOX 的“重要的缺陷”都要求在财务报告相关的内部控制报告中进行披露,在实务中将两者认为是一样的。总而言之,“重大缺陷”或“重要的缺陷”即可认为“内部控制失效”。

中国财政部办公厅发布的《企业内部控制评价指引》(征求意见稿)将问题点定义为“重大缺陷”、“重要缺陷”和“一般缺陷”三类,基本上承袭了美国 SOX 法案。

第十一章　财务决算(2):合并报表

“使用针对集团整体的规程来强化控制”的思路

合并报表过程中需要的内部控制:为了适当地开展合并报表决算,是否已配置相应的流程和人员

接着第十章单体公司财务决算的话题,在第十一章,我们来说合并报表。如果合并报表一旦出差错,业务流程和单体财务决算中产生、累计的各种财务数字就可能不得不废掉复位,所以这是美国 SOX 法案和日本版 SOX 中最受人瞩目的业务流程之一。

由于不是每个人都会接触合并报表,所以相比单体财务决算,它更加容易倾向于依赖个人。并且由于合并需要特有的专业知识,所以这个工作更倾向于依赖外部审计师。

具体来说,常见的情况就是,会做合并报表的财务人员一个人几乎处理了所有事情,也没有任何人进行实质性的复核。考虑到确保正确性、可交接性等,公司其实有必要从质和量上来配置双重复核的人才。

在实务中,公司先结束单体财务决算后,在进行合并报表工作的同时,外部审计师进入公司开始进行针对单体财务决算的审计,这种情况比较多。然后(本来外部审计师正在进行单体财务决算的审计),外部审计师一边对合并报表的判断和分录进行复核,一边编制调整事项。正如第

十章所述,外部审计师就应当要彻底“外部”,不能担当公司内部控制的一部分职责。公司必须明确制定合并分录和合并报表程序及工作流程,并且通过和外部审计师“事先商量”获取信息。

合并报表处理的关键点:关联交易确认,合并报表编制及集团会计规程

▼ 关联公司交易的确认和合并对象的判断

公司应当首先在单体财务决算的过程中识别关联方交易。然后,由于在合并报表中需要披露和母公司、子公司及兄弟公司的交易以及和公司的董事或高层管理人员的交易等必要信息,所以需要将其和一般交易区分开。

有了这些信息,在合并报表中公司再加入内部交易的抵销分录后,以此披露关联方交易。这里最重要的程序就是,决定这些对象中(子公司、与其有实质关系的关联公司、有股权投资关系的其他单位等)的哪些公司需要合并、哪些不需要合并,也就是合并对象的判断。可以不夸张地说,近年来大规模的报表粉饰事件中必定牵扯到合并范围的问题。

美国的安然事件中,安然公司通过将增加的负债和不良资产进行回租、卖出选择权等高级金融技术,将其转入不合并的特别目的公司,让合并报表上业绩好看了很多。

日本活力门事件中,问题出在通过股权投资组合进行交易。随之,为了亡羊补牢,日本业已更改了会计准则,来进一步明确关于股权投资组合合并的控制力标准和影响力标准。嘉娜宝事件中,就 15 家公司被不当地排除在合并范围之外进行了财务报告的调整。

首先,设立识别关联方的内部控制机制和组织很重要。比如,可以考虑将信息系统的交易方、资金借入方、投资方使用主文档来管理,然后在系统中设定对方是否关联方的标志,并且定期进行重新评估。

并且，对于对方是否属于合并对象、是否属于披露对象之类的判断，理应使用书面完整记录并获批准。并且与前述的“重要的判断”相当，企业最好通过独立的岗位或者部门进行复核。

▼ 制作、接受合并报表财务数据汇总表

单体财务决算的“信息收集”过程是，公司从各种各样的信息系统和业务流程中收集财务决算必需的财务会计数值；在合并报表中，这个过程就变成了从各子公司接受合并报表财务数据汇总表的程序。这个程序从步骤上来说可能比较简单，实则为深奥的流程。

首先，在子公司制作合并报表财务数据汇总表时，如果财务人员没有准备一张“财务信息归集表”，来说明财务数字如何从单体财务报表归并到合并报表的财务数据要求项，而只是将数字逐一填入合并报表财务数据汇总表中，这样的话，无人可以客观地复核这个填写过程中的恰当性。就算母公司提供了足够的指引，来说明如何将单体财务报表中各会计科目的数字一一放入合并报表财务数据汇总表的项目中，但是每个会计科目属于什么性质，通常，财务人员不在现场的话很难掌握。

母公司和子公司间，特别在一个国家内，最好能够统一会计科目体系(Chart of Accounts)，否则就需要制作和更新这张财务信息归集表。公司应当使得其各子公司能够制作出从该子公司会计科目体系层面变化到合并报表财务数据汇总表的归集表。

与之关联的另一个问题是，子公司因当地的法规要求而制作和提交的财务报表，如果在合并报表财务数据汇总表提交总部后再追加调整，则会使得报告给母公司的数字和该子公司最终的财务报表存在差异。这种调整最多的来自于子公司跟进当地外部审计师的调整分录；另外也会来自于那些需要早结账的公司，可能会有关账之后的若干重要交易。

从子公司单体财务决算的话题来说，单体财务决算的最终试算平衡表最好能和关账后加入调整分录的最终财务报表一致。由于某些信息系统会在关账后不能接受调整分录，所以需要通过其他方法完整地制作和

批准这些期后调整的一览表。

合并报表财务数据汇总表通常是从最终试算平衡表出发制作而成的。无论如何,应就合并报表财务数据汇总表与子公司最终的财务报表的重要差异向母公司报告,讨论是否需要进行合并报表上的调整(如果赶上合并报表工作正在进行中,则是否在合并报表中录入;如果赶不上的话,是否作为期后事项处理)。

最后,从母公司合并报表的观点来看,因为子公司在合并报表财务数据汇总表填写的内容将汇总至集团的合并财务报表,所以子公司应该有责任人对其报表数据进行最终复核和批准。

▼ 合并差异的调整

对于各子公司的合并报表财务数据汇总表及母公司的单体财务决算的结果,合并范围内间交易需要互相抵销,但由于各种原因往往会出现一定的差异。这里从内部控制的角度强调,需要明文规定的是对于多少金额、何种程度的合并差异要进行调查并调整。

公司在日常每个业务流程中,一旦发现差异,就应立即调查并解决小金额的差异。但对于合并报表层面的差异,即使存在相当大的金额差异,往往会由于未特别明文规定,财务担当者会凭着自己的判断,记入母公司的账进行处理。

并且,如果差异的理由是由于在途交易等正常发生的话,可在发生时进行处理就行。但是如果是由于认识不足或不恰当的流程原因造成的差异,就应寻求差异根本原因的解决方法。不仅限于差异,外部审计师往往会碰到因为子公司的财务人员认识不足,在每次的合并报表财务数据汇总表的填写中犯同样的错误。在这种情况下,只需通过达成共识等简单的对策就应该可以防止之后再犯错误。

▼ 集团会计规程

造成合并差异原因之一就是母公司和海外子公司所在地认可的会计

准则(GAAP)和公司对于选择、适用会计准则进行会计处理的不同。首先,以后者为例,母公司从海外子公司采购的情况中,母公司的采购确认基准和海外子公司的销售确认基准不同,在途商品肯定造成合并的差异。就算母公司和子公司都采用相应所在地的会计准则,如果集团间的贸易造成这样的'在途'差异的话就显得不太合理。

关于会计准则,海外和国内会计准则有多处不同。其中既有因集团间的交易造成的合并差异,也有由于会计准则的差异造成财务报表的不同。

由于国际财务报告准则(IFRS)及美国会计准则(US GAAP)要求集团内部的会计方针的统一,所以如果和当地的会计准则有重要差异的话,需要在合并报表财务数据汇总表中记录,或者通过合并调整分录来谋求会计方针的统一,不能对重要的差异置之不理。

在现行的日本会计准则下,理论上,同一环境下对于同一性质的交易应采用相同的会计处理,但实务上根据当地的会计准则制作的财务报表也可以直接用来合并,这也是欧美不接受日本的会计准则的最大的理由之一。所以,2008 年 4 月 1 日起(可提前适用)的合并事业年度中:(1)依据国际财务报告准则或者美国会计准则的情况下,可以利用合并报表程序;(2)这种情况下,如有对合并当期净利润有重大影响的会计处理差异的情况(合并上),必须修改子公司的会计处理。

同样,中国新企业会计准则第 20 号《企业合并》中也规定了在企业合并中,"被合并方采用的会计政策与合并方不一致的,合并方在合并日应当按照本企业会计政策对被合并方的财务报表相关项目进行调整,在此基础上按照本准则规定确认"。也就是说,中国企业如果有作为合并对象的海外子公司或分支机构的话,应该将按照适用的所在国家或地区的准则编报的数字调整为依中国准则编报的数字。

亚洲很多国家都是采用'基于国际财务报告准则'的会计准则,需要注意的是,它们并不一定和国际财务报告基准完全一致。

粗略分类,子公司所在国家的会计准则差异的调整有两种方法。

海外子公司较少的情况下,母公司可能理解该子公司当地的会计准则和会计处理,并且进行修正。

然而,如果海外子公司较多的情况下,如果要母公司分别理解各地的会计基准较难,所以各子公司应当在了解该子公司需要调整的内容后,相应地建立内控程序和组织。

于是,本节的标题"集团会计规程"就登场了。欧美的大型国际企业往往有数百页的会计政策,如果子公司采用的会计和会计政策不一致就需要向母公司汇报。这个和中国企业或日本企业的财务制度中常见的"财务理念"之类含糊的内容不同,应当要规定公司采用的收入确认基准、滞库商品减值评价基准等具体的会计处理。也就是说,母公司依据的会计准则应作为会计处理原则记录在会计政策中,让各子公司来把握和报告当地的会计准则和会计处理与"集团会计规程"的偏离。

有的企业将财务、总务等全面管理,甚至伦理、经营方针等全公司层面的内容也包括在内,可以制成500页左右的规章汇编集。大家可能会认为500页的数量相当庞大,但其实作为一个国际企业集团,能将所有子公司应该遵守的规章制度都归纳在这500页中已经是很了不起的了。

内部控制和规章、规定有着密切的关系。任何行为都需要按照明文规定来做,这样的想法可能有点过度,然而明文规定的规则毕竟还是内部控制的核心。一般来说,日本企业以及对于想进行海外发展的中国企业的集团层面控制,特别是对海外子公司控制较弱,先前的欧美企业可以作为有价值的例子供参考。

第十二章 税务管理

从性质上和金额上来看，公司承担多少税负这个问题是十分关键的

税金和内部控制：各种税法因国家和地区的不同而千差万别

“税金”的概念在经济及经营领域中由来已久。在原始农业耕作社会时期，就能够清晰地看到，为了满足公共利益的要求，从个人处征收钱财和物资，以确保达到最佳的整体利益。

税金有两个功能：其一是用纳税人上交的税来维持老百姓必要的开支以及建设并维护基础设施，换言之，即由受益者负担纳税；其二是所得收入以及社会财富的再分配，纳税人并不期待从中享受获取利益。日本的汽油税以及机动车重量税、中国的养路费等就是用来建设、保养道路的，是第一个功能的实例。当代的关税（让进口者缴税以保护国内产业）就是第二个功能的实例。

过去，封建统治者每年向农民征收贡赋，与其说是为了公共的利益，倒不如理解为是为了封建地主个人的权力。总之，“权力”和“税”是息息相关的。在当今社会，“税收”，这种维护收入以及社会财富的再分配的制度，是社会的重要组成部分之一（也可以说是顺应社会制度的发展方向，

产生了税收的制度)。例如,在日本,根据累进税率的税制,针对高收入者的税率较高(实际税率最高约 50%),而且遗产税的税率越高(超过 3 亿日元的部分为 50%,而在 1988 年以前超过 5 亿日元的部分为 75%),就越能缩小收入以及贫富的差距(这种税制的建立的初衷也可能是源自追求社会平等的文化背景)。在美国,所得税以及遗产税的各级累进税率差异较小,该做法鼓励人们通过个人努力去创造财富,并且认同社会的贫富差异。在中国的个人所得超额累进税率中,高收入者的适用税率较高(最高达 45%)。而遗产税也即将正式出台,草案中规定超过 1 000 万元的部分的税率高达 50%。目前遗产税在中国还未正式生效,这也许与中国重视从祖先那里承袭遗产的文化背景有关。

针对企业的税法主要是企业所得税。当企业所得税税率较高时,企业会在盈利较多的当年进行大规模的投资(税法允许抵扣的)。另一种情况是,针对企业销售收入征收相应比例的核定税额,这种税制是激励公司去谋取更多的利润,而不是鼓励企业去扩大规模。

▼ 针对税务的内部控制进行探讨的难度

第十章中提到,在美国 SOX 法案颁布之前,内部控制的某些方面并不为人所关注,其一就是"财务决算",其二就是这里的"税务"。

近年来,作为会计处理之本的会计准则以及相应的审计准则受全球化影响,各国的准则都在不断相互趋同。但是由于税务受到税法地域性的影响,各国的做法区别较大,需要很强的专业性知识。这正是在针对税务相关内部控制进行探讨时,碰到的最难的地方。

在欧洲,VAT(增值税)相关的税法非常复杂,会根据采购方、销售方的企业分类(一般企业、公共事业机关、个人等),而且因企业规模的不同,税率大不一样。甚至会复杂到,在针对电费的税率中,夜间电费对应的税率较低这样详细的程度。为了针对税制复杂这个现状,会计师事务所中成立了 VAT 的专业部门,其中根据税目不同还成立了各个专门的税务小组。

在美国，各个州和自治体的销售税（Sales Tax）的税率都不相同，因此孕育而生了很多咨询公司向企业提供税率等信息。此外，在美国还有一种替代最小赋税（Alternative Minimum Tax）的税种，这是一种强制性很大的税制，其目的主要是为了防止各个企业通过各种避税手段来降低其适用的法定实际税率。

所得税的计算 委托外部公司计算的结果必须进行复核

税法在各国千差万别，但大体上可以分为以所得税为代表的直接税和以增值税为代表的间接税。

此外，在税务流程中，一个明显特征是该流程的一部分或者是相当大一部分往往都会委托外部进行操作。

在了解了上述背景之后，我们一起来看一下税务流程中所要求的主要内部控制。

▼ 掌握影响所得税的各种因素

影响所得税的因素主要有以下几种：

（1）税法的修订。例如，中国从 2008 年起开始实施的新企业所得税法。对于内外资企业都有很大的影响。对有关税法进行修订时，需要考虑其对企业所得税的影响金额。

（2）会计准则的修订。会计准则进行修订时，如执行资产负债表债务法，就可能会对于递延税金（资产）等科目产生影响。

（3）发生新的交易。例如，设立新的海外子公司，发生所得时，需要考虑对其进行税前列支。

（4）引进新的税务规划战略时。例如，开始实施合并纳税时，需要考虑到其做法与之前的企业所得税计算的不同，对此需要做好准备。

公司为了正确地计算所得税，其前提是需要收集并掌握影响所得税

计算的信息，然后根据公司自身情况去判断分析。

上述(1)以及(2)的要求，类似财务决算流程的“对于会计准则的理解”，有时可以委托外部专家(税务师)的帮助。但是，为了防范重大错误的发生，最好还是能够进行有效的复核，由公司内部的人员掌握理解相关法律、行政法规、部门规章以及相关准则。

▼ 所得税计算

在实务操作中，公司经常使用计算软件等，生成计算表格(之后述及的“税金计算表格”)，计算所得税。

一般在税金计算表单中，建议输入以下项目：

(1) 会计利润以及应纳税所得额的调节表。

(2) 资产－负债账面价值和资产－负债的计税基础相互间差异的明细表。

(3) 所得税、递延税款资产－负债的计算表。

(4) 会计上必须录入的分录。

(5) 税率差异调节表。

税金计算流程的专业性强，宜分配给专人负责，且作为计算依据的税金计算表格必须经管理人员复核。此外税金计算表格在制作完成之后，一旦税法发生修订，或者公司涉足新的商业领域，都必须相应地进行更新。只有理解把握影响所得税计算的相关因素，并将其及时反映到税金计算表格中，确保税金计算表格与最新的税法等一致，才能够正确计算所得税。

在准备了最新版的税金计算表格之后，接下来就是录入相关必需信息，得出所得税的计算结果。

上述工作对已经执行新会计准则的中国企业来说，在计算递延税款以及申报企业所得税时，格外重要。

▼ 对于所得税计算结果的复核

所得税的计算无论是由公司内部人员操作还是委托外部人员进行操

作，都必须对其计算结果进行复核。

建议从以下几个方面着手复核：

（1）与前一期的内容进行比较。在复核会计利润和应纳税所得额调节表时，建议将本期的调节项目与前一期的内容进行比较。例如，前一期作为纳税调节项目，本期却没有进行调节的；此外，调节金额与前一期相比变动异常的项目，都是要复核的对象。通过这样的检查，经常可以发现税金计算的错误。

（2）法定适用税率与资产负债表债务法调整后的税率的差异。分析法定适用税率与资产负债表债务法调整后的实际税率的差异原因，从内部控制角度来看，也是至关重要的。可以通过分析税率差异的原因，发现那些输入项目等细节问题，以及那些通过计算复核也可能无法发现的错误。

（3）估计值的妥当性检查。近年来，越来越多的公司会在年底前提前关账，计算应纳税所得额时往往会用到估计值，以此计算所得税额。在这种情况下，估计值多少会与实际发生金额有所差异。应通过认真分析估计值和实际数之间的差异，确保不存在人为故意而导致差异的发生。此外，当某个项目的估计值和实际数之间存在较大差异时，很有可能是因为估计的方法有误，有必要重新检查估计的方法。

（4）对于应付所得税余额的分析。有必要针对前期计提的应付所得税余额，与申报后实际支付额之间的差异进行确认；如果差异重大，建议仔细分析差异原因。此外，还需要转回那些不该预提而错误预提的税额差异，避免过去的多预提所得税余额越积越大。

（5）对于递延税款资产的回收性分析。确认递延税款资产需要较高的专业知识，还需要考虑公司今后是否能够有足够盈利。企业一般对自己的未来业绩持积极态度，而与此相反，外部审计师通常会比较谨慎，两者之间经常会产生意见的不一致。公司和外部第三方的意见不合，本是难以避免的事情。从公司内部控制角度来分析，需要认真分析递延税款资产的收回可能性，并且需要由递延税款计算人员以外的其他人员对结

果进行客观的检查。

增值税的计算:需要识别应税项目

各国的间接税之间区别很大。前述的欧洲的情况相当复杂,中国的间接税主要以增值税、消费税、营业税为主,在税法中的地位也是举足轻重。日本的间接税以消费税为主,但由于征税基础是绝大部分的商品和服务,适用的税率都统一为5%,相对在日本的各税务中并不太重要,计算的手续也相对简单。

以下例子主要是从增值税(VAT)的角度出发,考虑相应的内部控制。

▼ 区别应税项和非应税项并且区别适用税率

在中国,填开专用发票并进行抵扣是增值税法规定的基础工作。营业税由于受行业不同,需要填开不同的专用发票。这一点从全世界各国情况来看,都是相当独特,且有中国特色的。

无论是根据旧会计准则或者根据新的会计准则,一方面,增值税销项税额的确认与销售的确认是同步的,体现了权责发生制的原则,公司根据该时点相应开出增值税发票。这点也是经常容易被混淆的概念。另一方面,虽然本来也是根据权责发生制的原则计入采购的,但在实务上,当公司没有收到增值税发票时,由于不能进行进项抵扣,所以一般都不在账面上确认增值税进项税额。但是在年末、季度末、月末,对于未收到增值税发票的货物,针对其应付账款,需要先计入应付账款暂估,从会计上明确采购交易的成立。

然后,在进行每笔交易时,销售时计入增值税(VAT)销项税额,采购时计入增值税项税额。

不管在哪个国家,为了正确计算增值税,最重要的是必须区分应税交

易和应税交易以外的其他项,以及区分所适用的税率。

现在一般都使用具有自动计算增值税的信息处理系统,系统通过识别交易是否应税,自动计算增值税。因此,为了确保在录入单据时能够正确区分应税项和非应税项,以及区分所适用的税率,事先设定主文档是非常重要的。由于欧洲的应税项目更加复杂,所以更有必要对主文档录入的准确性进行复核。

在中国,首先要区分应税和非应税项目,如房屋装修是非应税项目,飞机维修是应税项目 特别是在针对固定资产维修维护时,可能同时涉及增值税和营业税,需要清晰区分这两种情况。这个前提相当重要,关于应税范围的具体解释请参考章末注解[1]。

大多数公司销售或采购货物适用的税率都是 17%,因此可以通过设置主文档或每次交易时手工录入税率 但如果销售或采购的商品比较特殊,则应该在每次交易时识别相应货物判断其是否应税,且判断其适用税率。

关于录入增值税记账凭证的流程,已经在财务决算中述及,主要是对于凭证的复核和审批。

▼ 销项税额与进项税额的分析程序

一般情况下,针对账面的销项税与进项税余额,希望能够复核其入账的正确性。复核每一笔税金的计算正确与否显然是不现实的,所以针对销项税额与进项税额的账面余额,可以将应税交易总额乘以税率得出的结果与科目余额进行比较,确认两者间有无较大差异。建议每月都能执行这种分析性程序。

▼ 销项税额与进项税额的对冲

每个国家对于销项税额与进项税额的对冲都有不同的规定。中国的增值税法对于增值税进行税额的抵扣有严格规定。目前,增值税一般纳税人取得防伪税控系统开具的增值税专用发票、税务机关代开的增值税

专用发票以及废旧物资发票、海关完税凭证、运输发票、农产品收购发票的，可以抵扣进项税。总的一条原则是，除农产品收购发票外，其他发票必须自该开具之日起 90 天内进行认证、申报抵扣。部分企业时常会遗忘了认证发票，而导致不能抵扣，给企业造成了损失，因此在中国针对该点内部控制，更需要作为基础的业务流程认真实施。

税金业务流程的重要性：如果法定实际税率是 25%，则对利润将产生四分之一的影响

在上述各节中，讲解了涉及税金业务流程的主要内部控制。

下面提到的这一点一般没有包含在财务报告相关的内部控制中，而是近年来税务上的一个热门话题，就是转移定价。近年来各公司都逐渐重视转移定价的运用。当母公司在本国的各产品毛利与海外子公司同产品的毛利之间出现较大差异时，可能是公司有目的性地进行了避税而转移应税所得。母子公司间的所有交易额乘以百分之几，可能得出几亿元或者几十亿元的金额，如果公司被处罚追缴这样的数额，在税务上将是个十分巨大的风险。

如果公司遭到处罚，从内部控制角度来看，这将被视为公司当时公布了错误的财务报告，有时这可能被认为是内部控制上的一个缺陷。

很多国家都会要求公司整理保存有关转移定价的证明性文件。在中国新颁布的《企业所得税法》第 47 条规定："企业实施其他不具有合理商业目的的安排而减少其应纳税收入或者所得额的，税务机关有权按照合理方法调整。"至本书付梓之时，国家税务总局正在对《关联业务往来相关资料管理办法》(草案)征求意见，预计在近期内即将出台。该文件将具体规定纳税人进行年度所得税纳税申报时应向税务机关报送的资料，以及纳税人应按纳税年度准备、保存并按照税务机关要求提供的资料。这将增加企业对关联交易的举证责任，强化税务机关对转移定价的监管。各个企业也都在翘首期盼新的关联业务往来相关的资料管理办法的出

台。所以明确转移定价的设定方针，适当运用政策规避风险，这可能也是内部控制的必要的一个环节[2]。

美国 SOX 法案中，内控报告中的重大缺陷（Material Weakness），不少都涉及税务方面。日本版 SOX《实施标准》中，公司需要对与“公司经营目标相关的科目有关的流程”进行评价。仅仅为了支付税金而去开展公司经营的企业基本上是不可能存在的，从这种角度来看，税务流程和公司的经营业务并不相关。但是根据《实施标准》规定，“针对重要性较大的业务流程，可以将其作为评价项目，个别追加评价”。其中一个例子就是确认递延税金资产（负债）。

如果假设法定实际税率为 25%，对于税前利润的影响也将达到 25%。因此，在公司的财务报告环节中，其地位是举足轻重的。投资者对于企业现金流状况以及企业价值的关注由来已久。公司的实际税负多少，无论从性质上或者金额上来看，对于投资者来说都是需要进行关注的信息。由于美国 SOX 法案、日本版 SOX 和中国内部控制规范的目的就是为了保护投资者的利益，所以从这一方面考虑，对于税务流程进行评价也是必不可少的。

专栏　税金与会计

• 税务师与注册会计师职责上的差异

在第十二章中，述及税金有两个方面的功能（受益者负担赋税以及社会财富的再分配）。税务师作为税务专家，在其职责中体现了上述税金的两个方面。

税务师担负了监督企业和个人正确纳税的职责，并需要站在企业和个人的立场上，为其提供咨询服务。在美国，税务师提供合理避税服务后，如果所服务的客户发生损失，税务师会因为服务失职（Malpractice）而被投

诉，客户可以向税务师提出赔偿请求。

与税务师相比，注册会计师的职责只是合理确保财务报告的正确性。

作为注册会计师组织的会计师事务所在为企业提供正式咨询服务时，需要和审计合同分开，单独签订咨询服务合同。自从美国 SOX 法案实施以来，由于会计师事务所为客户提供咨询服务会影响其审计的独立性，政府制定并实施了各种各样的规章制度。

值得关注的是，欧美的会计师事务所原来的业务领域包含了“审计”、“税务”以及“咨询”服务，在美国 SOX 法案实施以后，各大会计师事务所都将“咨询”部门独立出原事务所，单独成立咨询公司。但是，咨询性质的税务服务却能够作为会计师事务所少数几项可提供的非审计业务之一得以保留[3]。在欧美传统观念中，会计师事务所会向客户提供审计以及税务两方面的服务，在审计业务中也需要税务专家的参与。与此不同，在日本，会计师事务所是禁止提供税务咨询服务的。

• 财务审计和税务调查

注册会计师和税务师由于都是专业人士，作为外部的第三方，两者对客户的拜访和工作程序方面经常会被拿来作比较。

作为公司而言，必须接受的是由外部审计师实施的财务审计和税务机构可能实施的税务调查（这里请先暂不考虑针对美国 SOX 法案和日本版 SOX 要求的内部控制的审计）。注册会计师是对财务报表的整体无重大错报漏报作出合理的保证；税务局的调查主要是选择易出现遗漏的申报项目，检查申报有无缺失。这是两者的最大的区别。

会计师事务所主要是从审计客户处获得报酬，这一点大大影响了会计师事务所的独立性，这也是在制定美国 SOX 法案过程中被讨论的最主要问题之一。在审计亏损企业以及站在盈亏临界点的企业时，更需要实施严格的审计程序；但实际上（也是当然的），外部审计师从这样的公司获取相应的审计报酬是相当困难的。所以会计师事务所在这一点上是最左右为难的。

税务调查的执行会因各国的习惯和规定不同而不同。

据说，在意大利有这样的制度(Condono)：如果按照税务机构要求的金额支付税款的话，过去一定年度账簿的税务调查就可以免除。因此，也就可以免除了双方实施和应对税务调查的程序和麻烦。在印尼等国家，是否需要进行税务调查，税务专管人员的判断还是起到了主要作用。

就像中国电影《至高无上》中，李雪健出演的税务稽查员老李兢兢业业、一丝不苟，面对金钱和物质的诱惑，毫不动摇。在日本电影《国税女稽查官》[4]中也同样刻画了国税稽查局的税官尽职尽责，不遗余力地去调查、发现各种问题，维护税法的尊严。这种国家权力机关也是维护社会健全和谐发展的重要组成之一。在电影《铁面无私》(*The Untouchables*)[5]中，芝加哥最大的黑帮被起诉有逃税嫌疑。老警员为了保护作为证人的黑帮财务负责人，展开了一场与黑帮的战斗。

税法是自古以来就有的制度，而财务审计制度是从当代起才逐渐开始。这两者是社会健全和谐发展必不可少的重要组成部分。

注

[1] 增值税的征税范围包括：销售和进口货物，提供加工及修理修配劳务。这里的货物是指有形动产，包括电力、热力、气体等，不包括不动产。加工是指受托加工货物，即委托方提供原料及主要材料，受托方按照委托方的要求制造货物并收取加工费的业务；修理修配是指受托对损伤和丧失功能的货物进行修复，使其恢复原状和功能的业务。

[2] 转移定价的相关税法规定，企业需要先与当地税务局确认集团内部的越境交易的价格计算方法，提交预约定价协议(Advance Pricing Agreement，APA)。

[3] 在同一会计师事务所中，为客户提供审计服务的同时，是禁止站在客户的立场上为客户提供税务规划的咨询服务的。

[4] 导演和编剧是伊丹十三。(原名“Marusaの女”，Marusa是日本国税

局稽查部的简称）影片描写了女税官和逃税者之间的各种斗争。该片荣获 1988 年第 11 界日本电影学院奖最佳影片奖。

[5]《铁面无私》（*The Untouchables*）的男主演肖恩·康纳利，凭这部影片荣获了 1987 年奥斯卡最佳男配角奖。

第十三章 人事薪资管理

企业以人为本

人事薪资的内部控制 批准计算依据以及复核计算结果的必要性

中国国家统计局的统计结果显示，2007 年中国的第三产业比例为 49.2%。伴随着经济的软件化进程，以软件开发企业、人力资源服务企业、医疗福利企业、学习培训企业等为主营业务的企业得以蓬勃发展。对于上述企业来说，人事薪资相关业务流程是非常重要的。

美国 SOX 法案中，人事薪资流程一般会被纳入评价范围。在中国，财政部办公厅出台的《企业内部控制应用指引》（征求意见稿）中也专门设置了“人力资源政策”的章节。

在日本版 SOX《实施标准》中，公司需要对与公司经营目的相关的会计科目有关的流程进行评价。因此，除了职工薪资所占比率较大的企业，许多企业并不将人事薪资相关的业务流程作为评价对象。但是，正所谓“企业以人为本”，不重视人事管理，就不成其为公司了。现按照内部控制的一般要求，对人事薪资流程进行探讨。

▼ 招聘录用和离职的手续

建议将招聘录用时应办理的所有手续归纳制作成检查一览表，在实

际招聘录用时，针对各个招聘者的实际情况，按照检查一览表中的项目，逐一进行检查，以确认经办手续无遗漏。该项目不仅限于人事部门内的手续，最好还包括招聘、离职时其他部门需要实施的重要事项。请参考如下示例内容。

- 要求应聘者必须提供的文件材料。
- 进行社会招聘时，根据招聘职位所需的要求，检查相应履历。尤其是，在将特定的工作经验作为招聘条件的情况下以及所招聘职位涉及内部控制的重要业务时，希望能向原用人单位了解核实该应聘人员在原单位的工作经历及其工作态度。
- 工作岗位描述书的制作、确认与保管。这种做法在中国和日本虽然并不多见，但在欧美，将各员工的职能和责任通过文字明确记载，制作成工作岗位描述书的情况十分普遍。尤其是针对财务决算、会计、资金、信息系统等需要职权分离的重要岗位，更是强烈建议编制相关员工的工作岗位描述书。在中国，《企业内部控制应用指引》（征求意见稿）中也强调了岗位说明制度的必要性。
- 进行入职培训。近年来，按照公司层面控制和信息系统整体控制的相关要求，越来越多的公司都在员工上岗时，对其进行职业道德和信息安全相关内容的培训。
- 员工卡的交付。
- 在公司的网络和信息系统中授予员工相应的用户名、向信息系统部门提出申请。
- 薪资主文档的登录。这是人事薪资流程中最重要的手续，如果是合同工，登录其小时工资；如果是正式员工，登录其月薪、年薪及各种补贴及扣除的依据等信息，并且应该对登录结果作双重检查。

公司也应该设计离职手续的检查表，在员工离职时予以执行。尤其是在中国，公司一般很重视实物的收回，如员工卡、未上缴的备用金、手提电脑等，但是往往会忽略“信息资产”的收回，例如网络和信息系统用户名

的停用、薪资主文档的删除等。上述几点从内部控制的观点来看，是很重要的。

▼ 考勤记录

薪资计算的前提是考勤记录。在制造业中，以产品为单位计算成本，根据工作日报告（时间）输入劳务费用，将其作为在产品余额的一部分，软件开发业等也将人工费用作为存货。

合同工是将工作时间与薪资计算直接挂钩的，正式公司员工也许只有平时的加班和休息日加班时，才对工资和补贴产生影响。无论是针对上述哪种情况，部门管理人员需要复核考勤记录的妥当性，确保记录正确且无遗漏。且有必要对平时加班和休息日加班进行事前批准，或事后的补批。

利用考勤卡和员工卡对员工进出办公室记录时，需要复核、批准可能产生的忘打卡或代打卡的情况。同时通过对部门员工的工作负荷量进行再确认，如果记录的加班时间短于直观认识，此时，从合规性角度需考虑是否存在免费加班的情况是非常重要的。

此外，对于派遣员工（即与人力资源服务公司签约，派往特定公司工作的员工），公司不直接付给其薪资，而是将其作为劳务费支付给人力资源服务公司。在第六章已经述及，如果是对派遣员工依赖较大的行业，购买的劳务相当于采购的“入库”。建议确认派遣员工的工作时间是否正确记录，并向人力资源服务公司做准确的报告。

▼ 薪资的计算

参照考勤记录和薪资主文档计算薪资。有时会将该计算工作外包给其他公司，公司基本都会再对外包计算的结果进行复核。即使是公司自行计算，也需要人事部门等对薪资计算（或者支付）的结果进行复核。在复核中，通过将本期或者本年的数据与上月或上年同期作比较，确认有无异常的大金额支付情况发生。还可以将实际员工人数与计算时的人数进

行比较，通过分析，确认有无虚构的员工。

此外，薪资计算期间以 15 日和 25 日为截止日的情况较多，在月末和季末有必要计提未付薪资。根据美国（美国会计准则）和欧洲（国际财务报告准则）的情况，由于需要计提员工提供劳务所换取的带薪假期，因此对带薪休假管理簿的复核就变得很重要。

▼ 人事评价

实施贴切的人事评价是企业的活力之源。就此而言，这也是公司层面内部控制中的一部分。

但是不可能存在一种百分之百满足所有人期望的人事评价体系。每个人的观点不同，价值观也不同，因此绝对“公平”的人事评价也许只是种幻想。然而，“透明”的人事评价是有可能做到的。为了让人事评价更能够被接受，公司应当要制定更清晰明确的评价标准。

作为人事评价相关最佳实例之一，公司的中期计划从部门目标中得以体现，并将各部门的管理人员的目标设定为数值，更进一步分解，尽量将担当人员的目标也设定为数值，然后分别对其完成度进行评价实施目标管理。制定目标时，设定一些较客观的数值性指标，能够清晰明确地进行评价是很重要的。制定销售部门和制造部门的目标时，设定比较性的数值目标会相对容易；但是，管理部门也可以设定各种各样的对应于中心业务的客观目标。例如，信息系统部门可以设定系统使用率和新系统导入的完成日期，会计部门可以考虑设定外部审计时发现的结算错误数和金额。

什么都用数字来说话，可能让人觉得太现实。但是考虑到如何去评判自己和部门业务的核心价值，而且表现出自己的努力程度，并将目标完成度清晰地展现在众人的眼前，数字无疑是非常重要的！当然，公司可以在实际操作上围绕业务中心点设定目标，同时再将上下级的设定目标相整合。

此外，管理人员这个岗位需要很多判断，因此也容易造成设定的目标

内容含糊，一旦管理层设定的目标都很含糊的话，其下属设定的目标肯定更不明确。这里仅仅举个例子，针对较主观的目标如“对属下的体谅、理解”，也可以考虑设定其目标为“离职率××%以下”“针对“属下所受教育、培训”这个目标，可以设定为与部门业务相关职业资格、考试的合格数等。

▼ 奖金的计算

奖金的计算与薪资的计算相同，人事评价的结果作为其计算依据，需要经过批准。此外还建议对计算结果进行分析性复核。

为了提高企业组织的活力，从注重成果的角度考虑，许多企业在计算奖金时，一定程度上会受人事评价结果的影响。但是，对奖金的影响会成为一柄双刃剑。如果评价不是很清晰明了，且员工对其并不接受的话，不仅不能提高员工积极性，反而会导致员工士气的低落，对内部控制的实施也会产生较大影响。另一种做法是，将奖金与部门和公司的整体业绩挂钩，这样计算相对简单，且也能够显现其激励效果。

给予员工股票期权是一种不用支付现金而网罗人才的方法，在美国和日本IT泡沫时期比较流行。

根据2007年1月1日起开始实施的中国新会计准则《第11号——股份支付》的定义，企业授予职工的期权、认股权证等衍生工具或其他权益工具，对职工进行激励或补偿，以换取职工提供的服务，实质上属于职工薪资的组成部分。所以，在会计处理上，应将其确认为职工薪资费用。而且，由于是与股价高低挂钩的报酬，因此在预计股价无法上升时股权激励的效果并不明显。但考虑到该方法能使企业利益相关目标与员工个人目标保持一致，所以如果能妥善运用的话，依然会是种有效的奖励手段。

另一方面，如果过度将经营业绩与管理层高额薪资挂钩的话，会增加管理层粉饰财务报表的风险，必须要注意如何保持平衡。这个也是在评价公司层面内部控制有效性时，需要考虑的事项之一。

▼ 年金的管理

根据劳动和社会保障部颁布的于2004年5月1日起实施的《企业年

金试行办法》中的定义，在中国的企业，年金主要是指企业及其职工在依法参加基本养老保险的基础上，自愿建立的补充养老保险制度。建立企业年金，应当按照本办法的规定执行。根据有关调查报告显示，截至2007年底全国有3万多家企业建立了企业年金。中国的企业年金制度选择了确定缴费型(Defined Contribution)的信托模式，引入了受托机构、账户管理人、托管人、投资管理人等多个角色。

在美国基本采用变动给付型的年金政策，但在日本，年金政策仍然以确定给付型(Defined Benefit)为主。

在日本的人事薪资业务流程中，确定给付型企业退休金的相关会计处理，从金额或性质上来看，可能是比较重要的。离职补偿金的提存不足会在预计平均工作年限内有规律地摊销，换言之，摊销年数是由企业自行衡量的。此外，离职补偿金与基金未来受益有关，会受基金预期收益率的影响，因此难免会有主观判断的成分。

通常，年金资产的使用和退休金的数学计算本身外包给信托银行和保险公司，公司有必要对该计算结果进行复核。当然并不是要复算年金数学计算的详细过程，只是要执行一定的分析性程序，尤其是要确保使用的折扣率、期望收益率、费用的分摊年份的正确，不得随意变更。如第十章结算中所述，接受独立第三方的复核也是一种值得推荐的方法。

此外，如果是委托金融机构，通常可以获得对其内部控制的外部评价报告[1]。

注

[1] 在美国，该报告根据SAS70法案(*Statement on Auditing Standards No. 70* "Service Organizations"(1992. 12))编制。在日本，则是根据审计准则委员会第18号决议"外包业务相关控制风险的评价"进行编制的。

第十四章　公司层面控制

管理层有没有“绝不做假”的决心？

公司层面控制的重要性和难点：如果“公司层面控制无效”，实务工作将面临巨大挑战

从各个角度来看，“公司层面控制”无论是在美国 SOX 法案、日本版 SOX，还是中国的内部控制体系中，都是最重要的领域。

首先，从美国的安然事件、世通事件，日本的嘉娜宝事件、活力门事件和中国的银广夏事件等近年来发生的一系列粉饰财务报表事件来看，企业是否对其财务报表做假，根本上往往取决于管理层的意识。“公司层面控制”，即是管理层是否拥有“我们公司的财务报表中绝不存在虚假记载”的决心，以及管理层是否努力营造实事求是的企业控制环境，并构筑相应的体制。

其次，日本版 SOX《实施标准》规定了首先要评价公司层面控制[1]，并根据其结果选定需要进行评价的企业分支机构。比如，“如果公司层面控制评价结果为有效，那么可以选择公司合并基础上销售额的大约 2/3 的分支机构”。此外，正如《实施标准》中同样提到的，“如果公司层面控制无效，必须扩大评价范围和追加评价程序”。

美国 SOX 法案中，《审计准则第 2 号》（简称 AS2）也要求最先对公司

层面控制实施评价，而《审计准则第 5 号》（简称 AS5）从以风险导向方法（Risk Approach）的视点出发，记载了如下表述："审计师可以根据对公司层面上的控制实施评价的结果，增加或减少对其他控制实施的测试程序（AS5 第 22 段）"；"公司层面的控制对其他控制的有效性起到监督作用。（略）运行如果有效，审计师可能同意削减一部分其他控制的测试程序（AS5 第 24 段）"。当初，有一些公司选择了 95％的分支机构作为评价对象。如果评价范围如此之大，将带来极为繁重的工作量。

中国的《企业内部控制评价指引》（征求意见稿）第十三条中，就内部控制的评价范围有如下表述："被评价单位内部控制是否在风险评价的基础上涵盖了企业层面的风险和所有重要的业务流程层面的风险。"《企业内部控制鉴证指引》（征求意见稿）第二十条中有如下表述："注册会计师应当测试企业是否存在对内部控制具有重要影响且有效的企业层面控制。注册会计师对企业层面控制的评价能够增加或减少其本应对其他控制进行的测试。"

▼ 相对于美国而言，中国和日本有弱化所有权和经营权分离的倾向

公司层面控制虽然极其重要，但其对应工作相当的困难。

第一，一提及公司层面控制，多数人就会联想到美国的公司治理及其他和经营管理相关的行为习惯。比如，美国 SOX 法案中要求董事会和审计委员会在监督公司运营中发挥重要作用。然而，较之美国企业而言，中国和日本企业存在弱化所有权和经营权分离的倾向。也就是说，中国和日本企业在公司层面控制方面，尚有很大的改进空间。但是，到底该实行什么样的公司层面控制，仍然很难断言。

笔者所属的会计师事务所的工作模板列举了 200 余条相关项目，有些项目只是举例，不一定需要全部执行。与之相反，美国 SOX 法案的审计标准中虽然只列示了 7 个项目，这些也是举例而已，除此之外尚有很多必要的项目。

日本版 SOX《实施标准》中列举了 42 项"和财务报告相关的公司层

面控制评价项目举例”[2]。虽然《实施标准》中使用了“例如”的字眼，还提出了“就公司层面控制而言，应参考列出的这42项，如发现问题，必要时应予以纠正”。在实务上，《实施标准》中所列的这些项目，应该是日本企业将来努力的方向。

中国的《企业内部控制基本规范》第十一条到四十七条这37条列举了中国大中型企业应有的公司层面控制的内容。

评价公司层面控制的第二个难点，是如何审定金额的影响。比如，评价中发现“缺乏道德准则或类似政策性文件”的问题，应该没有人能够说出该问题会对哪个会计科目产生多大金额的影响吧。外部审计师通常更关注会计科目的余额，因此他们很难仅仅因为公司层面控制的缺陷，就断言财务报告有关的内部控制有“重大缺陷”。何况，公司层面控制的不完善，主要都源于管理层的意识或者努力不足，所以外部审计师较难作出这样的判断。不过，如果在会计科目余额审计中发现的错误记录是由于相关公司层面控制的缺陷而导致的，那么也很有可能被认定为“重大缺陷”。

公司层面控制的具体举例：现已实施的控制方法已经涵盖了控制的很大一部分

笔者所属的会计师事务所的工作模板和日本版SOX《实施标准》所列示的项目中，颇多描述趋于抽象，但也有许多项目与中国和日本企业的实际经营管理中方法比较接近。然而，仍然有很多控制点值得导入、强化，或为了能够实施客观的评价而加以改善。

那么，让我们以多数企业实施的内部控制活动为中心，看一看公司层面应具备的内部控制的例子。作为参考，表14-1至表14-4列示了内部控制构成要素相关项目。这些仅是笔者根据经验列举的较常见的公司层面控制，而不是该层面应有的全部控制。

表 14-1　公司层面的政策、制度

公司层面控制举例	说　　明	内部控制构成要素
经营理念(Vision) 经营目标(Mission)	比如，列示公司的存在价值；公司应该追求怎样的优势和特长，并随之为社会和利益相关者做出怎样的贡献。	控制环境
道德准则、行为规范	通过培训项目促进知识普及和教育；对于违反道德的行为是否采取适当的措施。	控制环境
集团会计制度	(参见第十一章“合并决算”)	控制环境 信息与沟通
集团 IT 政策	公司常见的是安全措施和 IT 制度等。除此之外，还需规定信息系统开发和变更时公司须从职责分离和安全保障等内部控制的角度出发进行研究。	IT 的对应、信息与沟通

表 14-2　评价公司层面的计划和完成情况

公司层面控制举例	说　　明	内部控制构成要素
中期计划、预算	全公司及各部门的目标以财务数据的形式设定，根据完成情况定期修正目标，并分析偏离目标的原因并决定应对的策略。	信息与沟通
月度决算、试算表	适当的管理层审阅并使用内部财务报告。	信息与沟通
IT 战略	制定信息技术相关战略，使之与全公司的中期计划相一致(一部分亦可)。尤其须反映财务报告与内部控制的相关要求。	IT 的对应、信息与沟通
风险评估	企业须定期执行包括财务报告风险在内的整体风险评估。	风险评估与对应

表 14-3　组织、人事

公司层面控制举例	说　　明	内部控制构成要素
经营管理会议	会议定期召开，会议中审核、决定的内容都以书面形式留档。监事和财务报告职能相关负责人参加实际决定企业经营方针的会议。	信息与沟通

续表

公司层面控制举例	说　明	内部控制构成要素
组织结构图	显示了公司所构筑的必要的组织结构，明示下级组织向上级组织的报告关系。同时，该组织结构能够被适时更新。	控制环境 控制活动
审批制度、权限规则	明确何等职位或职责的经营管理者，拥有何等的权限。	控制环境 控制活动
职责分工制度	企业须明文规定职责分工，明确内部控制中重要的职责，比如决算、会计、资金、IT 等方面的负责人和执行人。	控制活动
岗位说明书	尽量明文描述所有员工的岗位职责。这样的做法在中国和日本还比较不普遍，尤其是财务决算和 IT 相关领域亟须加强。	控制环境
人事考评	企业须公正适当地进行人事考评。请参照第十三章“人事薪酬管理”。	控制环境
决算制度	企业须保有足够数量的具备决算工作能力的人才。请参照第十章“单体决算”和第十一章“合并决算”。	控制环境

表 14-4　监事、内部审计职能和通报制度

公司层面控制举例	说　明	内部控制构成要素
监事	由精通财务报告和内部控制的适当人士担任，发挥对公司经营的监督职能。同时，监事应与内部审计师和外部审计师进行沟通。	控制环境、监督
内部审计职能	须具备独立性，审计范围不受限制，并可直接向管理层、监事（会）报告。母公司和主要的子公司，须配备足够素质和数量的、能在全集团范围内实施监督职能的人才。	监督
内部控制的评价	定期对内部控制进行评价，向管理层报告评价结果并对发现的问题进行改进。此点是在各国内部控制法规下必须每年实施的活动。	控制活动 IT 的对应 监督

续表

公司层面控制举例	说　　明	内部控制构成要素
内部举报制度	与一般的报告路径不同，对于和财务报告相关的舞弊、违规违法、有悖道德规范的行为，应设立向独立的组织机构报告的制度，并在实际工作中可得以运用。举报行为应不受管理层掌控，举报内容应被妥善处理，同时防止对举报人可能的利益侵害。	信息与沟通 控制环境 监督
外部举报制度	这也与一般的接受外部信息的窗口不同。例如供应商可以将舞弊、违规违法等行为向采购部门以外的独立的组织机构报告。	信息与沟通 监督
防止舞弊	作为风险评估的一部分或者单独实施。研究是否有发生舞弊的动机和环境，是否引入了抑制和防止舞弊发生的控制制度。	风险评估与对应

公司层面控制的文件化和评价：对于集团整体，以统一的政策和制度实施控制

▼ 公司层面控制文件化和评价工作的注意点

一旦公司层面控制被评价为“无效”，在实务中将带来很大的麻烦。当然，从根本说，公司必须改进内部控制缺陷，将内部控制以书面文件形式记录（文件化）并对其实施评价工作也是必不可少的。

公司层面控制的文件化和评价工作实务中，笔者认为值得注意的是，由于与单个票据处理等单纯的流程层面内控不同，公司层面的控制具有更高层次的内容，公司必须下一番苦功确定各控制点。

比如，公司规章制度中写明“对于必要的组织机能，设置相应的部门并配备负责人，在组织结构图中明示并适时予以更新。”这时，在实际运行状况的评价（测试）时，可能会发现管理人员的人事调动情况没有及时反映在组织机构图中的错误（运行方面的缺陷）。如果内部控制设计为“……组织结构图每月更新”，实际运行的话，在实际评价工作中，就可能

可以避免这样的运行缺陷。

还有一例。公司明文规定“制定道德规范，以全部管理层为对象展开道德和合规性培训。”评价时，随机抽取管理职位的人员询问其是否接受了培训，即使公司严格要求培训，如果抽取 25 人询问，即有可能会发现其中几人实际未参加培训。如此说来，“公司制定了道德规范并可供阅读”这样的测试就似乎稍显不足。假如规定设定为“制定道德规范，面向管理层展开道德和合规性培训，参加培训人数比例达到九成（姑且不论九成是否足够）”，那么作为控制测试，可以追查是否参加培训比例达到九成的相关资料和实际参加培训的记录，以此为依据。

▼ 公司层面控制文件化和评价的形式

大多数企业集团的母公司都建立并运行了上面列举的公司层面控制（暂且不论有没有改进的空间），但是所有子公司是不是都和其母公司一样建立和运行了这些控制呢？

公司层面控制的文件化和评价，可按照每一个企业分支机构或每一个个别的内部控制，采取以下不同的形式：

（1）由母公司实施公司层面控制的内控文件记录，然后在所有分支机构实施评价。

（2）由母公司实施公司层面控制的内控文件记录，并由母公司实施对所有分支机构的评价。

（3）在各分支机构实施内控制度的内控文件记录并评价。

一般来说，公司层面控制会广泛影响公司全体，是以公司全体为对象的内部控制，因此以集团整体统一的规则实施的控制，应该由母公司实施记录内控文件的工作。关于评价工作，原则上应在各分支机构开展对于集团整体内部控制的评价，也就是说，应该在各个分支机构评价控制活动是否按照母公司的设计运行。（上述(1)）

另一个例子是，假使是“定期实施风险评估”的公司层面控制活动，子公司风险评估的结果会报告给母公司，则可以由母公司统一实施对结果

的抽样测试。（上述(2)）

相反，正如“员工的人事考核”，虽然有时由母公司制定考核目标，但在大多数情况下，具体的控制设计（Design）不得不由公司各分支机构做出。（上述(3)）

所以，对于就公司层面控制设定的各个评价项目，需要结合实际判断其属于上述的(1)、(2)、(3)中的哪种情况。

然而，企业应适时明文规定并宣传公司的政策，并积极促进集团整体的同一性。换言之，企业应通过规章制度和统一的方针，谋求集团整体在内部控制方面的步调一致。

注

[1] 美国 SOX 法案的《审计准则》中，最初规定了须评价“Company Level Control”。其意图是要求外部审计师“对于集团整体有效的内部控制进行评价”。

对此，日本版 SOX《实施标准》更注重于管理层层面，即“公司层面控制”。而且“在认识到独特的历史、习惯和组织结构后，可只以每个子公司和事业部等为对象，评价公司层面的内部控制”，所以（集团整体控制的有效性自不待言）“要求就管理层对公司层面的内部控制有效性作出评价”。

两者的差异之处在于日本企业就集团整体实施统一控制的倾向较弱。然而，美国 SOX 法案相应的 Company Level Control 也是以全公司的内部控制为中心的，即使有在个别子公司评价公司层面控制的情况，在实务中美国和日本的对应也基本相同。

[2] 日本版 SOX《实施标准》中，针对“内部控制的基本框架”中内部控制的各要素，列举了控制环境 13 个、风险评估 4 个、控制活动 7 个、信息与传达 6 个、监督 7 个、IT 反馈 5 个，共计 42 个项目。其中，就控制环境、风险评估、控制活动、信息与传达、监督这几个要素是 COSO

报告中定义了的内部控制要素。日本版 SOX 的《实施标准》，是在此基础上增加了“IT 反馈”。

中国的《企业内部控制基本规范》同样也承袭了 COSO 的理念，定义了 5 个内部控制要素，其中列举了内部环境 9 个、风险评估 8 个、控制活动 10 个、信息与沟通 6 个、内部监督 4 个，共计 37 个项目。

第十五章　信息系统整体控制(1)：信息安全

信息系统是企业运作不可欠缺的组成部分

信息系统(IT)和内部控制：在IT领域中，内部控制的层次参差不齐

现代企业的运作中，信息系统是必不可少的。即使认为企业的主要活动都是利用信息系统来进行的也不为过吧[1]。

目前，包括信息系统部门的工作人员在内，很多人对计算机的认识还停留在“不十分了解”的阶段。除导入美国SOX法案或日本版SOX的企业或取得了BS7799／ISO／IEC17799等[2]认证的企业以外，大家对IT领域的内部控制需要达到何种目标，仍然知之甚少。

IT领域的现状，与IT自身发展历史尚短有着直接的联系。与业务流程相关的内部控制至少已经经历了100多年的发展；而商用计算机系统在一般企业中的普及，如果从1964年IBM-360发售以来算起，两者之间的差距显而易见。

▼ IT内控的标准化与实务中的参差不齐并存

虽然与IT有关的内部控制的发展历史不长，但是换一个角度来看，IT内部控制的标准化已经波及全球。以注册会计师为例，基本上各个国

家乃至各个州都有自己认可的资格，而且取得资格的条件和考试等都各不相同。与之相对应，跟信息系统相关的内部控制专业资格比较统一，其中出名的是由ISACA（国际信息系统审计与控制协会）认定的CISA（国际信息系统审计师）资格。ISACA每年举办2次CISA资格考试，在全球约70个国家180个城市进行。

在业务流程的内部控制方面，虽然COSO[3]和PCAOB[4]都发布了含有有些具体示例的内控标准，但实务操作中，各个会计师事务所还是会参考和使用自己编制的标准模版。针对这一现象，全面包罗各项IT内部控制的COBIT[5]体系为众人熟知。

在日本，根据IT领域内部控制的要求，经济产业省发布了《系统管理基准》作为日本版SOX的补充内容。

中国财政部发布的《企业内部控制应用指引》（征求意见稿）中，也为信息系统一般控制单独设置了一个章节加以规定。

将目光转回实务，IT领域内部控制层次参差不齐的现象还非常明显。在业务流程中，实地盘存、授信管理等概念已经深入人心（是否认真地执行另当别论）。而就IT而言，我们却常常碰到在不顾信息安全的状态下进行系统开发的情况。当然如金融机构等非常重视信息安全系统体系构筑的公司也是存在的。

信息系统（IT）整体控制和信息系统（IT）业务处理控制：信息系统整体控制是衡量“信息系统整体是否可信赖”的机制

IT业务处理控制（Application Control），即指在业务流程中使用的个别信息系统[6]所包含的控制功能。例如，“当超过授信额度时，系统自动拒绝新订单的输入”就是IT业务控制的一种。另外也有系统处理和人为干预（手工处理）相结合的业务处理控制形式，如，“系统输出所有超过授信额度接受的订单的一览表，管理者对一览表进行复核”。

与业务处理控制相对应的，用来衡量“信息系统整体是否可信赖”的

是信息系统整体控制(中国财政部的《企业内部控制应用指引》(征求意见稿)称之为"信息系统一般控制")。举例而言,主要有用户账号和密码设定的安全管理、与系统开发相关的程序测试和开发成果确认等重要的内部控制。这些控制并不局限于某个特定的信息系统,而是统管信息系统整体的通用规则。通俗地说,就是信息系统部门日常所进行的一般业务管理。

例如,最常见的问题是访问权限的适当性。信息系统上的访问权限设定,通常都被理解为是信息系统整体控制管理的范畴。不过什么样的业务担当需要被授予何种适当的信息系统访问权限,则是由各个业务部门的负责人根据权责分工和业务效率的综合考虑决定的。

话虽如此,目前用户账号和访问权限的授予、变更、删除等(无论是由信息系统部门执行,还是由用户部门执行),还是被包括在信息系统整体控制的范畴之内。

▼ IT 业务处理控制是在各个业务流程中进行评价的

在这里需要提醒大家注意的是,在实务层面,美国 SOX 法案、日本版 SOX 和中国内部控制法规中的 IT 业务处理控制都是在各个业务流程中进行评价的。

信息系统部门和身为用户的业务部门的沟通有时会发生分歧(事实上,部门与部门之间的分歧是常常发生的)。从用户的角度看,会认为信息系统部门根本不知道业务的需要(如,为什么信息部门不能更实时地上传信息),而信息系统部门则会觉得用户对系统并不理解(如,用户应该对数据库表格的结构多加了解,这样就能区分数据提取的难易程度)。虽然部门之间存在各种分歧,但是身为用户还是有必要对自己业务上所使用的信息系统功能的工作原理有所了解。

如今,在美国 SOX 法案、日本版 SOX 和中国内部控制法规的实务操作中,IT 业务处理控制的评价通常是由业务流程的负责人和 IT 内部控制的专家分工、协作共同完成的。

此外，在对内部控制进行测试时，为了确定手工控制是否遵循了既定的内控规则，每年我们都需要对业务流程（不存在轮换测试流程的情况下）通过抽取样本的方式来评价内部控制的运行情况。而对于系统自动处理的控制而言，如果该功能没有发生改变且信息系统整体控制有效的话，则可以直接利用上一年的测试结果。

信息安全领域要求的内部控制：最重要的控制——用户账号、权限管理和密码设定

让我们再来看看信息系统整体控制所包含的主要内部控制。在接下来的内容当中，可能会出现一些平时不常见的信息系统用语。对这些系统用语我们可以不必深究，主要以了解相关的内部控制为主。

在信息系统整体控制体系中，与财务报告相关的主要有三大领域，其中“信息安全管理”[7]和“开发、维护管理”比较重要，另一块内容是“应用管理”。其他的“IT 战略和计划”、“IT 风险评估”和“业务持续性计划”等领域的内容一般被认为与财务报告的关系不大，不过其中有一部分控制会被包括在公司层面控制范围之中。

下面，让我们先从常见的信息安全管理领域开始介绍。

▼ 密码设定的基本要素

说起信息安全，通常都会联想到“密码”。为用户的账号设定适当的密码是确保信息安全的重要环节（稍后还会讲到用户账号和访问权限的关系）。一般在用户接入网络时会被要求输入密码（该密码通常是 Windows 或 Mac 等操作系统要求的[8][9]），然后在使用个别业务的应用系统（信息系统）时也会被要求输入密码。网络以及业务应用系统的密码应包含的主要要素如下：

- 定期变更密码

密码必须定期变更。一般至少每 3 个月变更一次，建议每月变更。

· 密码字符长度

一般的密码建议长度是 6 位以上,对风险较高的信息系统或功能而言,建议使用 8 位以上的密码。

· 使用文字字符

在密码中,建议同时包括阿拉伯字母的大写、小写和数字,最好还能加上特殊字符(%、&、!、*等)组成复杂的密码。

· 密码历史记录

如果变更后的密码,是前不久已经使用过的密码的话,结果跟没有变更密码差不多。因此,建议不要使用最近 10 次使用过的密码。

▼ 密码设定示例

我们就以一个容易记忆的强密码为例,向大家说明:

"KH100%jiayou!"

(这里的 KH 是作者姓名的缩写,"jiayou"是"加油"的拼音。不过这并不是作者实际使用的密码。)

如上所述,密码需要定期变更、字符长度要增加、须使用复杂密码、不能重复过去使用过的密码,而且网络和应用程序需要不同的密码,使用多个应用程序的话也往往需要用不同的密码[10]。还有,公司内网的公告牌、培训系统,公司以外的银行 ATM、证券公司账号、网上社区等都会使用到密码,可以说我们的生活中密码无处不在。但这些密码的长度、允许使用的字符等的要求不同,即使想用一些容易记的强密码,也不一定能够适用。

所以绝大多数的用户都会觉得"这么多复杂密码,记不住!"然而,这样一来,有人就会由于密码记不住而写在便签上贴在电脑显示器旁,这是不行的。

当然保存密码的最佳方法是全部记住,但是如果实在没办法记的话,可以采用如下的次优方案。

把自己使用的密码记录在 Word 文档中,对该 Word 文档加上密码。

这样一来，只要记住网络接入密码和 Word 文档的密码就可以了。需要注意的是，Word 文档不能使用“密码”等字样作为文件名。

▼ 与密码相关的常见问题

业务应用系统的密码功能不完善，是常见的密码相关问题。例如，现在日本的银行现金卡密码只允许 4 位数字，由于很多用户使用生日（典型的弱密码）作为密码，使得盗用银行现金卡的现象增多。因此，对于重要的应用程序而言，如果没有定期变更密码、设置最低密码长度以及使用复杂字符的功能的话，应该对系统加以修改，或通过别的方法加以完善。而信息系统管理部门需定期发布通知，提醒用户进行密码变更。对一定期间未更改密码的用户，加入跟踪复核清单进行监督。在信息安全管理政策中或信息安全标准的规定中加入最低密码长度限制以及使用复杂字符等的规定，要求用户遵照执行。

有些应用程序的信息安全管理员（或在系统上拥有很大权限的管理员）有权查看所有用户的密码，在用户忘记密码的时候可以帮其找回密码。这样的做法虽然方便，但是对于信息安全来说是非常不妥的。这种情况下，信息安全管理员应该进行密码初始化操作，由用户自行登录并重设密码。初始化的密码建议也采用系统随机生成的密码，避免每次都采用同样的密码。

▼ 用户账号和访问权限的赋予、变更、删除

用户账号的创建、访问权限（如设定能否使用订单的输入、修改、确认等个别功能）的赋予和变更等，必须按照相关业务部门和人事部门的确认执行。比较理想的做法是，事先根据职务分工的要求确定各项职务所必需的系统功能，而信息系统部门只需根据人事部门发布的特定职位的人员录用、变动通知，在系统中按照该职位事先确定的访问权限进行设定即可。不过一般的做法是由业务部门填写用户账号和访问权限的申请书，信息部门按照该申请进行相关的设定。

另外,我们常常会发现公司的系统中保留有一些不需要的用户账号。及时地删除那些已经离职的职员用户账号是非常必要的。在欧美国家,如果要解雇一位在系统上拥有很大权限的管理人员或职员时,会事先禁用该人员在系统上的用户账号,然后再将解雇的消息通知本人。这样一来,可以有效地避免恶意的系统信息破坏行为。因此,如果由于密码输入错误而无法登录时,当事人可能第一反应是‘我是不是被解雇了?”

▼ 用户账号和访问权限的定期复核

对用户账号和访问权限的状态,要求实施定期的复核工作。复核的主要目的包括如下几点 确认失效的用户账号是否已经删除、职位变动的员工权限是否已经更新、访问权限的授予情况是否和职务分工的要求相符等。

目前执行访问权限适当性复核的公司很少。即便要执行的话,势必将用户部门也牵扯进来。因此,访问权限适当性复核是信息安全领域比较难处理的问题之一。

通常部门内部各职员权限会由业务部门的管理人员来确认。对小规模公司而言,很可能直接由管理负责人来确认。无论如何,最理想的做法还是如前所述的,如果能够事先确定各项职务所需要的具体功能,则访问权限的定期复核所要做的就是再确认这些定义是否适当即可。

▼ 授予特定的用户账号

对用户账号必须注意的要点是,共享用户账号的做法是不允许的,每个用户都应该被赋予特定的用户账号。究其原因,是由于用户账号如果共享的话,势必造成密码也是共享的,而且即使有系统日志[11]存在,也无法确定到底是谁登录了系统进行了操作。话虽如此,由于目前很多 ERP 系统的用户账号使用许可证的价格很高,所以将具有通用权限的账号进行共享的情况比较常见。如果存在共享账号的情况,有必要明确地定义共享的目的和共享账号的权限,并由管理层进行确认。另外,共享账号如

果被赋予了只读以外的具有修改的功能的话，一旦有人员职位变动、离职的情况出现，就必须立即进行密码变更处理。

▼ 管理员账号

如前所述的信息安全要素对普通用户以外的账号也同样适用，尤其是系统管理员的账号。该账号的使用频率和使用人员都非常少，因此对该账号的管理通常都比较马虎。但由于该账号被赋予了很高的权限，所以才更应该加以良好的管理。除了系统管理员账号以外，服务器操作系统、数据库、系统软件[12]等的管理员账号也需要加以足够的重视。

由于访问权限的设置必须限定在业务所需的功能范围内，因此管理员账号的访问权限原则上也被限定在日常业务所需要的功能范围之内。如果是具有极高权限的非常用账户，其密码应写在纸上装入信封封存，并放在金库中加以保管。对于供应商提供的缺省用户账户（在软件开发时加入的用户账号），如果没有使用必要的话，建议将其禁用或删除。特别是 ERP 系统，它涵盖包括财务会计在内的各个业务范围，而其超级用户的初始密码一般广为人知，因此需加以足够的重视。

▼ 信息资产的物理安全

对计算机房的访问必须加以适当的限制，建议对进出机房实行登记管理。机房内部的温度、湿度须进行适当的调节，并配备必要的灭火设备。相反地，如果将重要的应用服务器放在积满灰尘的办公室角落里的话，则是严重违反了物理安全的要求。

▼ 其他

信息安全领域所要求的其他内部控制罗列如下：

- 信息安全政策（方针）、信息安全标准。将公司对信息安全有关的想法、密码和用户账号的管理原则、信息系统相关的重要定义书面化，并对公司员工进行相关的培训教育，做到众所周知。

- 计算机病毒对策。公司的每台电脑、服务器都必须加装防病毒软件,并定期更新病毒库。此外,相关的防火墙[13]的导入和配置也很重要。
- 日志。根据信息安全政策的要求、业务的需要程度,对风险较高的系统功能的使用和总要信息的修改等操作,进行日志记录管理。
- 信息安全事件的监控(需关注的与信息安全有关的事件,如反复的登录失败、晚间使用高风险的业务功能、没有更新计划的数据被更新了)。信息安全事件也需要根据业务上的需要程度和风险因素,来加以监控。

专栏　来自信息系统审计师的感慨

• 涉及 IT 领域的问题很难估计其影响程度

各个企业与 IT 相关的内部控制各不相同,而且负责审计的信息系统审计师所拥有的经历、擅长的领域和思路也各不相同。就连笔者本人也不例外,虽然在系统软件包的实施咨询和系统开发方面比较有经验,但是谈到防火墙的设定的话,心里还是没底。

每个认为自己是个系统专家(更准确地说,是专门挑刺的专家)的人都会认为自己公司的系统存在缺陷,但说到具体的缺陷内容,可能就会出现各种各样的不同回答,如"按 ESC 键却不能关闭当前界面[14]"、"通过远程登录的方式进行数据交换很差"、"界面的设计缺乏美感"等等。

信息系统审计师的主要工作之一,就是作为财务审计的一环,对信息系统整体控制进行评价。

说到要分析信息系统整体控制领域中存在的缺陷(将在第十七章具体介绍)到底会以何种形式、在多大程度上对财务会计数据产生影响,有时候是非常困难的。例如,服务器机房的进出情况没有留下记录,该缺陷到底会对什么会计科目产生多大的影响是非常难以说明的(感觉上好像根本没

有影响)。但是也有一些其他缺陷,如管理员用户账号如果使用弱密码的话,服务器上的数据库遭到直接破坏的可能性就大大增加,对财务数据的安全性产生直接的影响。

• 实际尝试模拟黑客攻击的服务

正如第四章所说的,在业务流程的内部控制失效的情况下,会直接造成期末财务审计时抽取的样本量增加。在信息系统整体控制失效的情况下,系统审计人员会得出"计算机输出的凭证可信程度值得怀疑"或"不能依赖IT业务处理的控制"等含糊的结论,这就有让审计人员(与信息系统审计人相对的、对财务报告进行审计的会计师事务所的主要队伍)和客户无法理解系统审计的意义何在的倾向。

话虽如此,信息系统仍然是当代企业不可欠缺的组成部分,而且其重要性也在日益提高,因此对信息系统相关的内部控制进行评价也就成了理所当然的事。会计师事务所也在不断地修改审计手册,强化IT相关的内部控制评价的内容。

有的时候,同事会提出这样的要求:"既然是做系统审计的,那就教教我Excel的用法吧!"虽然是系统审计师,但也不一定对于Excel很熟悉;当然,如果具有一定的编程知识的话,对掌握Excel中函数的使用,会比较有帮助。

笔者所属部门内,除了进行通常的信息系统审计业务的审计师以外,还有钻研更深层次信息安全的专家。为了确认公司是否具有足够的黑客防范能力,他们甚至会提供实际进行模拟黑客攻击的服务。这样的信息安全专家通过可监控无线局域网数据流的软件,嘟哝道:"啊,看见某某的文件的!"这听上去确实让人觉得有些恐怖。

[1] 美国的COSO框架(参看第一章注释1)中的内部控制基本要素包括

五个组成部分:(1)控制环境;(2)风险评估;(3)控制活动;(4)信息和传递;(5)监督。COSO框架中,将与IT相关的内容都包括在了"信息与沟通"这一章节中。日本版SOX《实施标准》中,为了强调信息技术的重要性,将"IT反馈"单独作为内部控制的基本要素之一来考虑,因此一共包含了六个组成部分。中国的《企业内部控制基本规范》中,将基本要素分为(1)内部环境;(2)风险评估;(3)控制活动;(4)信息与沟通;(5)内部监督五项,基本与COSO框架相一致。

[2] BS7799是英国标准协会(British Standards Institute,BSI)于1995年2月制定的关于信息安全的标准。2000年12月,BS7799中的第一部分被ISO采纳,正式成为ISO/IEC17799标准。

[3] 1992年美国COSO委员会(the Committee of Sponsoring Organizations of the Treadway Commission)发布的报告,是与内部控制相关的事实上的世界标准。

[4] PCAOB(Public Company Accounting Oversight Board)是SEC(美国证券交易委员会)的下属机构,是负责制定以美国SOX法案为基础的内部控制审计标准以及对会计师事务所进行监督的机构。

[5] COBIT(Control Objectives for Information and Related Technology)。截至2007年1月,发布的最新版本是2005年末的COBIT4.0版。由美国IT治理协会发行,该协会与ISACA(信息系统控制协会)的关系密切。在COBIT的项目中,还有专为美国SOX法案筛选出的COBIT for SOX (IT Control Objectives for Sarbanes-Oxley)。

[6] 信息系统、应用程序、软件、程序等,都是些相近的用语。由于这些名词过于基本,因此在普通的IT用语辞典中不一定能查到。总的来说,上述名词是按照从大到小的顺序排列的。信息系统是涵盖公司各个业务领域的整合应用程序。应用程序是人们为了特定的目的(业务管理、表格计算、游戏等)而使用的软件。软件是相对于硬件而言的,它是程序和数据的整体。这里所说的软件是指在系统内部工作的、实现特定功能的程序群。

[7] 日本版 SOX《实施标准》中列举了与财务报告相关的 IT 整体控制的评价对象，包括“IT 的开发、维护管理”、“系统的应用管理”、“内外部访问管理等的系统安全保障”、“外包相关的合同管理”等四大领域。其中第三项“内外部访问管理等的系统安全保障”就是信息安全的不同说法。

COBIT 的体系包括，“计划和组织”、“取得和导入”（基本上与开发、维护相当）、“交付和支持”（外包的管理、信息安全、帮助台、应用等）、“监督和评价”等领域。可见，COBIT 所涵盖的不仅包括信息系统整体控制，还有其他更广的领域。

[8] Windows 和 Mac 分别是微软和苹果公司开发的操作系统软件[注 9]。网络连接指的是，通过有线或无线的方式将电脑、路由器等设备连接起来，并加装相关的通信软件的整个过程。“接入网络”是指，打开电脑让 Windows 或 Mac 等操作系统（OS）启动，直到电脑达到可使用的状态，并且通过服务器的识别，使得电脑能够与服务器或其他电脑进行通信的状态。

[9] 操作系统（OS）是对计算机整体进行管理的基本软件，其基本功能包括键盘输入、图像输出、磁盘和内存管理等。电脑以硬件为基础、以系统软件为平台，在此基础上运行各种应用程序和软件。

[10] 单点登录，即指网络和主要的信息系统使用共同的密码，用户只要一次登录后就可获得相关的访问权限。有些软件甚至允许同时登录到网页界面。这样做虽然很方便，但是随着单点登录的范围扩大，信息安全却被降低了。

[11] 日志分为很多种，有访问日志（记录登录、注销的情况），有命令日志（记录用户使用了什么功能），还有更新日志（记录什么数据被更新了）等。根据不同的目的，适用的日志也不同。针对高风险的功能，命令日志比较合适；而针对重要的数据，就要用更新日志。

[12] 参考第十六章“系统软件的变更管理”的注释。

[13] 防火墙的作用是防止公司的计算机网络遭受来自外部的非法入侵。

防火墙主要通过以下几种方式实现:在服务器上安装防火墙软件,使用具有防火墙功能的路由器,使用专用的硬件防火墙。

[14] 以前,Windows 的应用程序一般都可以通过 ESC 键来关闭当前的界面。此外,在一个电影描述中提到,ESC 键被设计成是触发计算机病毒的条件。

第十六章　信息系统整体控制(2)：开发、维护

出错的不是计算机而是人

IT 领域的内部控制所要求的职责分工“信息安全管理员”、“用户”、“开发人员”的分工

在开始讨论开发、维护的话题之前，先谈一些 IT 相关业务所要求的职责分工问题。

职责分工在信息系统整体控制中也是非常重要的。不过这一点也跟其他 IT 相关的内部控制一样，没有得到普遍的认识。

IT 领域的职责分工中，最重要的是“信息安全管理员”、“用户”和“开发人员”的相互独立。

通常信息安全管理员的主要任务是创建、修改、删除用户账号和访问权限。除此以外，还有在第十五章中介绍过的统管信息安全相关的内部控制、向公司员工宣传信息安全政策等职责。

大家一般都会认为用户保持独立性是理所当然的事。不过在用户部门掌握信息系统构建主导权的公司，常常会发现他们直接在用户部门中设置了账号管理人员，由其对用户账号和访问权限进行创建、修改、删除等处理。这样一来(虽然要考虑该管理员同时兼任何种业务职能)，信息安全管理员和用户这两个角色之间就没有做到相互独立。信息安全管理员可以擅自更改自己的权限，或者创建虚构的用户进行登录，给凭证的管

理或客户关系的管理等业务职能带来很高的风险。

有时信息系统部门的工作员工在开发自己负责的系统的同时，还需要为用户提供技术支持，因此会在生产环境[1]系统上拥有全部的权限。这样的情况是实施美国 SOX 法案和日本版 SOX 过程中遇到的最严重的 IT 职责分工问题。从业务角度上说，由系统开发人员亲自担任生产环境的系统支持的话，确实可以提高不少效率，不过这是非常危险的。如果系统开发人员直接修改生产环境程序的话，就是可以对系统中的数据进行任何操作。

因此，在 IT 部门设置另外一个“运行维护员”的独立角色就可以满足职责分工的要求。运行维护人员负责对系统的运行情况和批处理(在十七章具体介绍)的执行情况进行监控，以及执行用户支持和帮助台的职能[2]。原则上，开发人员不允许拥有生产环境的访问权，而是应由运行维护人员进行生产环境的管理。有时运行维护人员也负责生产环境的用户账号和访问权限的授予、修改和删除。

信息系统部门最理想的组织结构是建立横跨所有系统的开发组、运行维护组和信息安全管理员(组)。相反，如果只按照每个应用业务系统来设置分组的话，无论如何都会削弱职务之间的分工。

如果系统开发人员为了系统支持的目的而必须访问生产环境的话，应该将他的权限设定为只读。如需要进行生产环境数据的直接变更，或系统异常终止时的应急程序变更时，就应与运行维护人员一起，或用非常用的应急管理员账号进行处理。

如果公司一定要让开发人员拥有生产环境登录、修改权限的话，就必须用日志记录所有其在生产环境中的操作，并由信息安全管理员或适当的管理层进行复核。

▼ 小规模 IT 部门的职责分工

在大规模企业的 IT 部门，应该实施的职责分工还有很多，但这里让我们来看看，如何在小规模的 IT 组织中实现最低限度的职责分工。

IT 相关业务的一大特征就是外包往往很多。有的公司的 IT 部门甚至只配置 1 名管理人员和 1 名员工，其他的所有业务都外包。

这种情况下，一般由 IT 职员负责用户账户和访问权限的授予、变更和删除（信息安全管理员）。管理人员负责对开发和应用的相关事项进行审批，如果信息安全管理员不在的时候，代理其职能。至于编程、测试等开发工作，都通过外包来完成。

笔者曾经遇到过如下身兼数职的事例。有一位外部咨询人员在帮助企业导入财务会计系统之后，凭借着对该系统的了解和管理能力，转行到该公司担任会计经理，并且继续负责用户账号管理、访问权限管理和用户支持的工作，同时也拥有系统开发的权限。这样一来就身兼了三项主要应该独立的职务，而且其本人还是一位非常重要的用户（会计经理）。

开发、维护领域的内部控制：“开发、变更要求的审批”，“测试的实施”，“开发变更结果的审批”

“开发”是指设计、导入新的系统，而“维护”指的是追加新系统功能、修正系统错误等工作。有时这两项工作被分别处理，但要求的内部控制基本相同。接着就让我们看看开发和维护领域所要求的内部控制。

▼ 开发、变更要求的审批

导入新系统的时候，或在系统追加新功能或功能变更的时候，会产生必需的工时和费用，而且在系统上进行的业务处理也会发生改变，因此管理层的审批也是必不可少的。通常，大规模的系统项目会作为投资来处理，根据公司与投资相关的规定进行审批。其中与 IT 相关的内部控制主要是对各项系统功能追加、变更的申请的控制。用户部门提出需求并确认，信息系统部门收到申请后，确定相关的工时、影响范围和优先顺序。

这里需要注意的是，信息系统部门内部发现的变更需求，如修改程序内部的错误等，是不存在用户部门申请的。在这种情况下，信息系统部门

内部就需要制作相关的申请，并落实审批。不管项目是否发生费用或用户部门是否负担费用，系统开发、变更的审批过程都必须完整地进行。

▼ 实施测试并保留测试结果

在审批用户需求之后，就可以开始制作系统设计书。大规模的系统开发、变更项目中，从定义用户需求(概念设计)开始，详细设计到编程说明书，不同的阶段都需要制作相应的文档。不过对于小规模的系统变更，可能就只需制作编程说明书。制作完善的文档固然重要，但是从内部控制的角度来看，测试的重要性更高[3]。在大规模的系统开发、变更项目中，对照相应阶段的设计书，必须进行从单元测试(程序层面测试)、整合测试到用户测试。而在小规模的变更中，可能只需进行单元测试就够了。

无论系统开发、变更项目的规模大小，单元测试都是必须进行的，因此应该保留可以有力证明系统程序的测试已经得到切实执行的内部控制证据资料。测试计划和相应的测试结果应该进行归档，例如，测试脚本(测试的顺序和内容)以及相关的确认标记等。测试中使用的详细数据通常不需要归档。相反，如果只在系统设计书中简单地描述“测试已完成”通常是不够的，需要有充分的证据，以使第三方信服所实施的测试内容是足够的。

▼ 开发结果的审批

开发好的程序在移送到正式生产环境之前，需要经过管理层的审批。作为之前没有提到的职责分工的重要一环，在移送的开始阶段就需要保证相关的职务独立性，移送实施人员不能是系统开发人员，而应该是运行维护人员或没有参与开发活动的管理员。审批开发结果的证据多种多样，其中由审批人员实施移送并保留相关的移送记录，可能是最切实的审批证据。另外，也有以单元测试结果为准留下审批证据的情况。

如果只在开发需求申请书上审批开发完成的话，容易出现问题。确实，针对需求而言程序的开发已经结束，特别是一旦通过了用户测试，就

可以说开发的结果已经得到了用户的认可。但是较大的系统变更时，可能会产生数十个乃至上百个程序的修改，而且会在系统正式上线后需要进行修改。针对这些追加修改，在原来的开发需求申请书上都进行再审批是不现实的。不过如果不进行任何形式的审批的话，就会出现程序的最终更新日（或编译日等）晚于开发完成审批日，这是必然引起信息系统审计师关注的情况。另外一个问题是，程序的编制、变更所对应的申请书也会变得难以追查，而可能需要仔细查看系统设计书。

因此，不仅针对每个被满足需求要出具审批，对程序整体而言，开发责任人也必须就开发的结果进行审批。

以上内容中出现的诸如开发需求审批、测试文档、开发结果的审批等，就是开发、维护领域中最重要的控制内容。

对 IT 开发、维护领域的内部控制进行评价的方法，主要就是抽取一定期间的程序变更样本，对相应的开发需求、测试实施、开发结果的审批等证据进行审查。

如果用上述方法对企业的开发、维护领域进行突击检查的话，不出现这样那样的问题的企业几乎没有。然而，要构建和维持可以信赖的信息系统的话，就需要对开发、维护领域进行有条不紊的管理。

▼ 数据库的变更管理

到此为止，我们的讨论是以程序的变更为前提的，而伴随着程序的变更，通常也会对数据库进行修改。数据库的变更管理主要也是三个方面的内容：开发和变更的需求审批、测试文档、变更结果的审批。只是根据不同的数据库，实务执行的方式有所变化。

在如 AS400[4] 的文件系统环境中，虽然程序对象和文件对象存在差别，但是系统和数据库的变更管理手续是一模一样的。

另一方面，如 Oracle[5] 数据库那种表格结构的情况下，数据库与应用程序相互独立，这就需要另外的管理手续对表格的追加和项目的追加变更等进行控制。这种情况下，就需要设置一位“数据库管理员”，负责审批

设计人员对表格的追加变更申请,并在获得批准的情况下实施变更;同时更新定义表格项目和名字的数据字典。因此,在测试的时候,通常是在测试应用程序变更的同时,对相关的使用到的数据库变更进行测试。

▼ 网络的变更管理

对网络的管理而言主要也是三项内容:需求审批、测试文档、变更结果的审批。然而,网络是通过网线或无线将服务器、客户端、路由器等设备连接起来,并安装上用于通讯的软件系统后,才组成一个完整的网络。所以网络的变更需要进行更具体的定义。

例如,"更新与网络相关的'网络结构图'和'防火墙配置表'的内容",这样的定义方式就很明确。需要补充的是,在更新这些文档的时候,必须将经过审批的最新版本和过去的版本一并保管。

再举一个例子。有时网络管理员的职责是管理与网络变更相关的申请和测试,以及实际执行变更工作。在这样的情况下,要准确地区分各种各样的变更是一件非常头疼的事。例如,与通信公司的合同属于外包相关的合同,购买通信设备属于硬件的管理和日常公司采购规范的范畴,网络管理软件的变更属于系统软件的整体变更等等。

由于网络变更的定义比较困难,因此信息系统审计师在确定总体样本的时候也很困难。通常是按照公司的定义确定总体样本。因此,公司如果实际上管理严谨,且为了能够实施有效管理内容而定义了相关内容并努力做到的话,在需求审批方面出的问题应该较少。

网络的变更测试中存在各种情况,从必须进行测试的项目(通信线路的更换),到不一定需要测试的项目(细小的设置变更)都有。还有网络设备的设置等,没有区分是测试环境还是生产环境,使得测试的证据和变更结果的审批含糊不清。

针对上面所定义的这些变更(在定义含糊的情况下,关注变更的实质内容),至少需要制作测试和导入的证明文档。最好可以设计一份网络变更管理专用的模板,将测试的内容和结果予以记录。然后对不需要测试

的情况下，记录下不予测试的理由。

▼ 系统软件的变更管理

对系统软件管理来说主要还是上述的三项内容：需求审批、测试文档、变更结果的审批。系统软件也被称为中间件。它的定义比较宽泛，包括操作系统、工作计划调度器、备份软件、反病毒软件、数据传输软件、网络管理软件、数据库管理软件、系统运行情况监控软件等等。

与应用程序和数据库的变更相比，系统软件的变更容易被轻视。但事实上，大型系统软件在操作系统补丁包或软件版本升级的时候一旦发生问题，可能使得在其平台之上的应用程序无法运行。因此，变更测试和审批也是必不可少的。

系统软件变更的定义和网络相似，也很困难。

作为明确定义的一个例子，在“系统软件一览表”中记录服务器安装的软件、软件版本以及补丁包等信息，这些信息需要更新。

最低要求也与网络相同，针对不同的变更定义（在定义含糊的情况下，关注变更的实质内容），需要审批和制作相应的测试和导入的证明文档。

这里所说的系统软件仅指在服务器端安装的软件，不包括个人电脑（客户端）安装的软件。对于个人电脑而言，我们主要关注的内容是有无安装非法软件、是否按照公司的规定安装软件、通过何种方法来确定软件安装的合规性等等（个人电脑的关注点与变更管理的关系不大）。

▼ 开发标准、开发方法

开发标准主要包括开发、维护相关的表格样式，以及程序的编码规则等。

编码规则是指，程序中函数的取名和定义方法，以及在程序中添加说明、作者、编程日期等附注的规则。如果不制定这样的规则，或者因为仓促而随意编写的话，几年之后再看的话，可能连本人也可能想不起当时编

码的内容了。平时根据编码规则进行程序开发的话，可以使日后的系统维护变得更加容易，所以，作为明文规定的规则，强烈希望公司能够归纳其编码规则。

在一般公司，大规模的系统开发比较少，所以不一定独立拥有完整的系统开发方法。但是，大型跨国公司或系统开发服务公司可能拥有这样的方法。

由于实施大型系统的时候，需要花费数千万乃至数亿的资金。为了防范失败的风险，就需要使用适当的项目管理方法来控制开发风险[6]。开发方法通常会包括如下内容：项目的各个阶段、阶段中的各个步骤、每个步骤产生的成果，以及步骤之间的前后关系和注意事项等。

[1] 生产环境是指处理实际业务数据的环境。与之相应地，开发程序的环境称为开发环境，开发完成后用来测试程序的称为测试环境。开发环境与测试环境可以合二为一，但是生产环境必须与开发、测试环境严格分离。

[2] “系统管理员”是称呼IT相关负责人员的词汇，不过每个公司对系统管理员职能的定义是不一样的。通常会被称为“XX系统的”系统管理员，以管理用户账号、访问权限和用户支持的工作为主，其他还有如开发与用户之间的联络员角色(系统分析师)、操作系统和数据库管理等工作。如果从IT职责分工的角度来看“系统管理员”的话，希望能够让负责操作系统和数据库管理的人员与其他的负责人员进行职务分离。本文中强调的“开发人员禁止访问生产环境”不仅指不能以用户身份访问应用程序，还包括不能拥有访问服务器操作系统和数据库的权限。

[3] 当开发日程急迫的时候，开发人员通常会优先选择程序的开发，而把设计书的制作延后。设计书最主要的目的是确保系统维护的可行

性，虽然不希望在开发过程中被延后，不过文档在制作时间方面还是有一定的余地的。然而，即使是紧急情况，也绝不能将未经过测试的程序移行到生产环境运行。

[4] AS400 是 IBM 公司出品的商用计算机，其主要特征是强化了企业业务处理的能力，是 Mainframe 业务系统的代表作。更换商标后，被称为 eServer iSeries。

[5] Oracle（甲骨文）公司的数据库软件，在大型系统中拥有压倒性的市场占有率。

[6] 已经公开的项目管理方法有如下几种：美国的非营利团体 PMI（Project Management Institute）制定的 PMBOK（Project Management Body of Knowledge），以及英国商务局开发的 Prince2（PRojects IN Controlled Environments，2nd version）。

第十七章　信息系统整体控制(3)：系统运行

系统环境的识别决定评价工作量

系统运行所要求的内部控制：确保程序在生产环境顺利运行

▼ 批处理的管理

批处理是指，信息系统内部执行的一组处理活动，通常由工作计划调度器(Job Scheduler)这类软件对批处理的进程进行管理。举例而言，每天自动打印发票、每月自动更新科目余额、每隔一小时刷新收到的订单和存货跌价准备等重复性的工作都属于批处理。如果批处理执行失败或者中途出错中止，很可能会对数据产生重大影响，因此必须加以良好的管理。

具体地说，首先工作计划调度器中新增或变更批处理的操作必须经过批准。可以用申请书进行审批，或者可以将最新的批处理任务清单输出，在清单上加以审批。

另外，批处理任务设定、变更的权限只能授予必要的负责人。根据生产环境访问权限的要求，程序开发人员是不能拥有该权限的。

对批处理任务的执行情况进行监控，一旦出现错误或异常中止的情

况，立即报告相关管理人员，并及时采取适当的应对措施。应对处理措施相关的证据形式多种多样，包括所有的处理结果都以日志的形式加以记录，异常发生时记录在系统运行检查表中，记录所采取的应对措施并由管理人员确认等等。有的公司还采用了自动手机邮件通知或短消息通知等方法，一旦出现了错误或警告时，可以立刻告知需采取相关的运行维护措施。

▼ 备份

当文件被误删除时，我们通常都会求助信息系统部门，让他们在备份中恢复被误删除的文件。对公司而言，如果重要的信息系统数据丢失的话，可能会引起很大的麻烦，因此进行适当的备份是非常重要的。例如，对医疗器械（心脏起搏器等）的制造企业来说，各个患者所使用的产品的编号是非常重要的数据，必须进行适当的备份。

数据备份文件需要定期进行测试，保证其确实可以用来恢复数据。我们常常会遇到不对备份数据进行恢复测试的情况，如果在实际需要恢复数据的时候，才发现数据读不出来或备份的磁带是空白的话，备份负责人员可就手足无措了。

备份数据要求进行异地保管，如日本这样地震多发地区，一般要求备份间隔距离在 50 千米以上。

以前，在荷兰发生过如下事例：

"2 楼？3 楼？"

公司："我们没有对备份数据进行异地保管，因为不可能有地震。"

审计："但是（荷兰）有可能发生洪水吧？"

公司："我们的机房在 2 楼，没关系。"

审计："2 楼也可能有风险。"

公司："不不，荷兰的 2 楼（G 楼→1 楼→2 楼）相当于日本的 3 楼啊。"

审计："这样啊……"

应用负责人员对公司存在不满情绪，蓄意对基干系统服务器和备份媒体进行破坏等情况也不能说不可能发生。所以为了避免风险，公司应该将备份资料进行异地保存，并且做到职责分离。

▼ 灾难恢复计划和业务持续计划

灾难恢复计划(Disaster Recovery Planning，DRP)和业务持续计划(Business Continuity Planning，BCP)与上文所提到的备份工作紧密相关。不过这两项内容通常被认为是与财务报告不直接相关的信息系统整体控制。

灾难恢复计划是指，实际发生数据丢失或服务器损坏时，根据事先制订的计划，进行恢复工作。灾难恢复计划所研究的主要内容包括 新服务器的调配、异地备份的取回、负责人的召集、实际恢复所需的时间等。

业务持续计划的范围更广，需要针对不同的情景，按照业务的重要程度，来限定恢复工作所要花费的时间，并制订相关的恢复计划。例如，金融机构等企业的决策通常是不允许有延迟的，因此通常都会设置一个拥有足够冗余的数据中心，来处理国内各个分支机构的业务数据。

不过灾难恢复计划和业务持续计划所涉及的内容不在应用的领域之内，与其说是信息系统整体控制，倒不如说是公司层面的内部控制来得贴切。

▼ 帮助台和服务级别

为用户提供适当的技术支持是十分重要的。

与此相关的公司 IT 服务级别，也需进行适当的监督。具体来说，从帮助台受理的询问次数和所花费的时间等数据，可以了解到信息系统的实际利用率和服务器的处理能力等基础信息，也会包含系统变更需求处理等系统维护领域的内容。将这些内容汇总，每月出具 IT 服务报告，提交给管理层审阅。

服务级别协议(Service Level Agreement,SLA)是将信息系统(目标)使用时间和帮助台的受理时间段等为用户部门提供服务有关的内容,与信息系统部门以书面的形式确定下来。SLA 在中国和日本并不多见,不过在欧美国家却常常可以看到。有些公司会将用户支持和基础设施的管理外包,这样的情况下,建议同时与受托方订立 SLA 协议。

IT 相关的外包合同:IT 外包需谨慎

日本版 SOX 的《实施标准》中,讲述了信息系统整体控制所要求的内部控制的内容。其中所举的第四个领域,就是"外包相关的合同管理"。在中国的《企业内部控制应用指引》(征求意见稿)中,也有一个章节专门讲述了"外包管理"的内容。

IT 业务的一大特征是经常外包。尤其在美国,外包更是习以为常。有些大胆的企业甚至将除了战略和计划以外的所有业务整个都外包了出去。而中国和日本的企业,通常只将应用和开发的业务进行外包。

在进行大规模外包之前,需要先确认受托方的相关信息,如成功的案例、业务能力、公司体制、应对变化的能力、财务状况、有无接受其他竞争对手的委托等等,判断对方是否足以信任。在作出外包的决定前,公司内部必须谨慎地进行审批,要防止在外包中止后相关职能无法在公司内部进行衔接的问题,或是发生经费失控的情况。

对小规模的外包而言,仅仅依靠通常的服务采购控制程序是不够的,建议能够增加 IT 服务相关的内部控制。

日本版 SOX 的《实施标准》中和美国 SOX 法案的实务中也包含相关内容,"必须对接受委托公司的内部控制的设计和运行情况进行评价确认"。因此,通常大型的 IT 相关业务受托公司都准备有其内部控制的外部评价报告[1]。所以在外包之前,建议先确认外部评价报告的相关内容。

评价信息系统整体控制的注意事项:内控设计上的缺陷对财务报告产生的影响难以评价

▼ 系统环境的识别

在前面的章节中,我们给大家介绍了信息系统整体控制所要求的主要内部控制。仅这些主要的内部控制,内容已经很多了。

然而,信息系统整体控制应根据不同的"系统环境"来进行评价。由于与系统有关的企业内部组织、规章、基础架构不同,需要识别不同的系统环境。我们应用一个例子加以说明。例如,公司开发的销售、采购、物流系统由系统部门进行管理;而财务系统使用的是市场上销售的软件包,由会计部门负责安装和管理。这样在进行信息系统整体控制评价时,就要分两个评价单位进行——"信息系统部门"和"会计部门"。

在十六章中,我们曾经提到过,"如果只按照应用业务系统来分组的话,无论如何都会削弱职务之间的分工"。问题不仅仅只在于职责分工,如果各个组之间的业务处理方法大不相同的话,就必须对每个组都进行一次信息系统整体控制评价。

如果对每个信息系统都分别进行信息系统整体控制评价的话,被评价的项目个数可能就会与全体业务流程的个数相当。在这种情况下,由于信息系统整体控制主要对财务报告产生间接的影响,如果将其作为评价的重点,可能让人觉得无法理解。

防止这些弊端出现的方法,我们已经在第十六章中提过了。那就是在组织中建立横跨各个系统的开发小组、应用小组、信息安全管理员(小组)等组织架构,统一信息系统的处理环境。这样一来,即使各个系统的架构不同,只要处在同一处理环境中,评价的过程就能简化。

也许有人认为,为了应对制度而大举改变业务流程本来就是本末倒置的方法,但分散管理各个系统也是不尽如人意的。因此,统一不同系统

相关的规则和管理体系，识别单一的系统环境无论是从内部控制评价的角度，还是内部管理的角度来说，都是值得推荐的。

▼ 独立业务应用系统[2]和表格计算软件的控制

在IT领域中，也有一些不作为“信息系统”对待的小规模（但比较重要的）的业务应用系统。

在第六章中提到的企业银行业务系统、第九章中的与资金相关的管理软件等，都属于小规模业务应用系统。这些系统通常都是安装在相关负责人员电脑中的，且不受信息系统部门的管理，不过，对财务报告而言，却有着不可忽视的重要影响。

如果不将该应用软件视为信息系统的话（如纸质的台账一样），可以不被纳入财务报告相关内部控制评价范围。相反地，如果属于信息系统，且构成了独立的计算机处理环境的话，就必须对其信息系统整体控制进行评价。

比较合适的处理办法是用公司制定的计算机处理环境规定进行统一管理（即，跟信息系统部门管辖的其他信息系统一样对待）。尤其需要关注的是密码、信息安全以及备份情况等基本要素。实际上，对于那些管理公司所有支付、贷款、金融衍生交易合同等的应用软件，如果存在用户账号和密码共享、密码位数是4位数、使用人员调动或离职后也没有进行密码变更等问题，无论这是否是制度评价对象，都不能放任不管。

即使在小规模业务系统中，也应将输入、复核、确认等权限适当地分配给各个用户。如果系统无法进行这样的权限设定，那么就必须通过增加手工控制来降低风险（如打印凭证进行确认、台账管理等）。

在开发、变更领域也许大部分不适用，但对应用程序开发商提供的程序补丁（修正软件错误的程序）或升级程序，可能按照开发维护系统的标准来对待较好。

另外，对于那些与财务会计关系密切的表格计算软件的管理方法，请参照上文的独立应用系统的相关内容[3]。

▼ 信息系统整体控制中的缺陷

确定了系统环境之后，就可以开始对内控进行评价了。通常信息系统整体控制是问题出得最多的一环，尤其是高风险缺陷(或者是控制缺失)的数量，有时可能比所有业务流程中发现的总和还多。看到这里，从事企业信息系统管理工作的读者们应该会觉得有点心慌吧。不过，正如在十五章中所提到的，IT 领域的内部控制的发展历史还很短。今后，在衡量风险和成本的基础上，逐步实现所要求的内部控制就可以了。

说起信息系统整体控制的缺陷的话，主要难点在于确定其对财务数据到底有多少影响(风险)。我们以开发、维护为例，假设在本期发生变更的程序中抽取样本，发现其中有半数的变更没有保留相关的测试证据，这种缺陷可能无从确定到底会对什么科目产生多大影响。不过，一旦系统中隐藏有漏洞致使财务数据出错的话，那就不能再置之不理了。

日本版 SOX 的实施标准中指出“信息系统整体控制的缺陷并不会直接产生虚假的财务报告事项，因此不必将其评价为重大缺陷。”不过同时又说到“即使在 IT 相关的业务处理控制设计良好的情况下，也有可能在实际运行过程中无法持续保持控制的有效性，使得产生虚假财务记录的风险增加。”

在美国 SOX 法案实施的时候，第一年度的内控报告中出现的“重大缺陷”中，有约 5％是与信息系统整体控制相关的问题[4]。

在信息化社会的今天，经营者需要在实际工作中努力地管理好支持企业运作的信息系统。

注

[1] 在美国，是根据 SAS70(*Statement on Auditing Standards No. 70* “Service Organizations”1992.12)出具的报告。在日本，是根据审计标准委员会报告第 18 号“委托业务相关的控制风险评价”出具的

报告。

[2] 登录电脑后，只有该电脑的用户才可以使用的应用程序。

[3] 日本经济产业省的信息系统管理标准补充中指出："即使是 EUC（终端用户计算 :表格计算软件生成的包含公式、宏、程序等的表格或数据库的管理软件），其与基本的信息系统管理方法是相同的。"

[4] 根据 EDGER Online，Inc. 的调查结果，截至 2005 年 5 月，美国 SOX 法案在正式执行的第 1 年末（2004 年度），总共 2 826 家企业中的 364 家（12.9%）被报告存在重大缺陷，这些缺陷中有 69 件（5%）直接与 IT 相关。

第十八章　内部控制项目的展开（1）：思路和计划

作为管理活动持续改进的契机来推进！

最后两章的讨论，是基于应对美国 SOX 法案、日本版 SOX，以及中国版“SOX”——《内部控制基本规范》的实际经验，循着通常内部控制项目的进展顺序，介绍重要的或值得注意的地方。此外，由于这三个内部控制法规的要求的差异点主要存在于评价范围、评价对象的确定等方面，所以在适用于评价对象的内部控制建立健全、书面文档化、管理层测试的实际操作，以及项目的计划、开展、确认等步骤上，基本没有太大的差异。

笔者希望可以把在项目过程中需要留意的关键点，尽可能地告诉需要应对各自国家的内部控制相关法律规章的公司或者担当部门。如果能够正确地应对内部控制相关法律规章，就可以比较经济地形成可见的显著成果，这样的项目担当人员就可以帮助公司获得成功。

内部控制相关法案对应的思路：保持适度余地，合理应对是明智之举

类似“为了美国 SOX 法案而花费的巨大费用和时间是公司的大负担”这样的言论非常多。所以，在日本版 SOX 以及中国版 SOX 形成的过程中，监管机构花了不少精力来考虑如何为公司减轻负担；但是，公司应

当清醒地意识到，不管怎样，还是会有一部分的时间和费用是不得不付出的。

由于不同国家的内部控制相关法案的目的都是为了确保财务报表的可信（或者说帮助恢复投资者信心），所以有些人会认为财务报告相关的内部控制中只要没有重大缺陷就可以了，但实际上这样的理解并不准确。确实，着眼于对财务报告有着重要影响的内部控制是非常重要的，但是，在美国 SOX 法案和日本版 SOX 的实务和中国版 SOX 的考虑中，金额是判断缺陷重要性最重要的标准。例如，实现 100 亿元税前利润的公司，重要性水平设定为税前利润的 5％的话，就是 5 亿元；只有在影响财务报表 5 亿元以上的内部控制缺陷才会被认为是重大缺陷。

这里最大的问题是，这么巨额的差错，在财务结账和报告流程、销售记账的基准、递延税款等会计处理环节可能不太会出现；但是，几百万元的错报和漏报就不认为是问题。这明显是不对的。

第一，公司通常是不会一直获得丰厚的利润的，在持续经营的前提下，利润“有波峰也有波谷”。那么同样一个内控的问题，在公司利润高的时候没问题，利润少的时候就有问题，这样怎么也不能说内控设计是有效的吧。

第二，“积小流以成江海”。对于同一个会计科目有影响的多个内控缺陷全部加起来考虑是对的。理论上，影响金额在几百万元的内控缺陷若在多个事业部或者子公司出现的情况下，就会构成重大缺陷。

第三，公司经常会有子公司分别上市，或者把某个事业部卖掉的情况。从这些子公司或者事业部来看，原来在公司整体所作的内控建设和评价的工作还是比较宏观，还无法完全适于这些将要独立的子公司单独“出海远航”。

第四，如果公司比其他公司准备内容更粗略的时候，实际一旦发生问题的时候，股东代表诉讼风险就将难以回避。而且，外部审计师有着金额导向性的思维，“一旦结果糟糕，那就一切都很糟”，即使有着在内控评价范围之外的财务记账上的错误，也很有可能把这点作为内控缺陷提出来。

如果考虑一下其他的法令或者风险的话,例如,“产品的安全性只要不导致消费者投诉就马马虎虎得了”、“建筑工程只要不违反环境法规就马马虎虎得了”,这样的态度是要不得的;只有留有适度余地的对应方法才是恰当的。

借着各国内部控制相关法案出台的契机,把通常需要考量的与财务报告相关的内部控制全面而清晰地检查一遍,识别内控缺陷和改进点,并积极加以应对整改,这其实已不仅限于法规的要求,而是作为公司管理也是必须要做的事情;而且改善成本不大或为零的话,通过持续改进来提升管理也是必然的!

内部控制项目的评估对象虽然限定在“与财务报告相关”,但也涵盖企业集团全体的内部控制。这是对公司有着积极意义的:既然好不容易花费了大量时间和费用,那就活用这个项目中的好的成果,切实地对管理活动开展持续改进。

计划阶段:作为公司整体应当评价的内容不能漏掉

毫无疑问,为了不枉费太多的费用和时间,根据恰当的项目计划逐步推进是非常重要的。

据说,美国版 SOX 法案给公司带来巨大负担的理由之一,是由于不少管理层考虑,通过向外部专家支付大额费用开展法案的应对,从而可以对管理层尽到应有关注义务、具备确切对策而提供证据,从而减轻股东代表诉讼的风险,在日本和中国,这样想的管理层应该比美国要少吧!

▼ 内部资源与外部资源

基本来说,利用内部资源需花费时间,利用外部资源则发生对外费用。而且,各国内部控制法规的准备工作,包括在第一年生效时的一次性工作(主要是文档化),以及从第二年开始的每年发生的持续工作(主要是

评价)。

如果过度依赖外部的资源,就无法培养公司内部掌握内部控制书面成果的维护和实施技能的人才。反过来说,只利用内部资源的话,特别在第一年,工作量将会很大,而且项目的方向性和评价的质量可能也是令人担心的一个话题。所以,最理想的状态是:从一开始将内外部的资源平衡和混合地使用,等到有些经验之后,再转向利用内部资源,这也最为顺畅。

▼ 内部资源的本质

许多公司在应对各国 SOX 法案的时候,内部的项目管理团队大致有以下三种方式来组合:

(1) 跨部门的项目组,即各部门均派人参加;

(2) 内部审计部门组成的项目组;

(3) 财务部门组成的项目组。

对项目成员来说,应当要具备两种能力:从内部控制审计的角度开展评价工作的方式和技能,以及能够从管理者和现场部门的角度考虑内部控制应该如何来构建的技能和实施能力。

内部控制评价的部分,与内部审计部门的工作非常接近。所以,内审部门紧密参与项目是理所当然的,一点不管、隔岸观火无疑是不行的;但另一方面,原本有着特定的专项审计目的的内部审计也是很重要的。在第十四章中,公司层面内部控制中也说到,企业必须保证有效的内部审计机制。企业需要好好地研究和探讨一下内审体制和机制的设立和长效管理,以满足为准备内部控制相关法案所发生的人工和时间,以及这之后持续评估所需发生的人工和时间的需要。

建立健全内部控制的部分,如果由内部审计部门来负责实施的话,这样就难免会在后续的审计中审自己建立的东西。所以,把建立健全内控的责任放在现场部门的负责人或者管理层是非常必要的。

另外,财务部门在建立内控的过程中,是实施与财务报告相关的内部控制的主角,而且也是各国内部控制相关法案中面对外部审计师的主要

负责部门,所以它对于项目的适度参与是不可或缺的。理想状态下,内审部门与财务部门一起牵头,其他部门派员参与,内审部门的代表掌管"内控评价",业务部门的代表主管"内控的建立健全",这种组合是最好的。

▼ 外部资源的本质

外部资源一般来说有着如下的组合:

(1) 从外部审计师那里,仅仅希望就项目推进等事宜获取免费建议;

(2) 在支付一定的报酬后,从外部审计师那里寻求建议;

(3) 外部审计师以外的外部资源,作为项目成员直接参与项目。

对外部审计师来说,如果企业采用恰当的应对方案,对内部控制审计相关的审计风险则可降低,所以外部审计师将会很乐意提供建议。换而言之,希望看到否定意见和拒绝发表意见的外部审计师是不存在的。但是,免费提供的意见还是有其局限性的。

从外部审计师那里得到的有偿建议,优缺点并存。优点自不用说,从审计师本身那里得到的支持,企业会比较放心。但是缺点呢,则是审计师尽管可以提改进建议,但是由于审计独立性的限制,既无法帮助管理层开展实施和决策,也不能代表管理层进行内部控制的测试和评价。这也是因为内部控制的设计、实施与运行的责任最终还是归于管理层。

此外中国版 SOX,即财政部等五部委出具的《企业内部控制基本规范》中明确要求,提供内控咨询的中介机构不得对这家公司同时开展内控审计。

于是,本应在完全准备好之后参加"正式考试"的企业,有时会请外部审计师开展内部控制审计的事先"模拟考",被称为"演习"(Dry Run)。

利用外部审计师以外的中介机构来开展内部控制相关法案应对的优缺点则与上述内容相反:尽管帮助管理层开展的准备工作没有内容上的限制,但由于不能预测外部审计师是以何种视角看待某个问题的,公司不得不在进行准备工作时抱谨慎态度。另一方面,外部审计师会根据是谁帮助公司开展内控评价,来判断对其的信赖程度。

日本版 SOX 的内部控制审计仅要求针对公司自身的内控评价发表意见(间接报告意见),而在美国和中国版的 SOX 要求的是直接意见,即对公司的内控是否有效发表意见。但不管审计师最终的意见如何,一般均要求"审计师为了对管理层的评价结果进行审计,应当实施必要的审计程序,获得审计证据"。如果内部控制的评价是由公司以外的独立第三方开展的话,较容易得到外部审计师更高程度的信赖。

▼ 评价对象和范围的选定

决定了资源的构成之后,下一步就是决定评价对象和确定工作范围。当然,需要的资源总量是由工作展开的方式所左右的。

关于评估范围的选定,美国 SOX 法案和日本版 SOX 所采用的方法有部分不同。

美国 SOX 法案在实务上,大致可以分以下几个程序:

- 首先,在合并财务报表上选择重要的会计科目。此时的重要性水平是以财务报表审计的重要性水平(比如税前利润的 5%)为基准,同时考虑定性的因素,大部分公司会选择八九成的会计科目作为对象。
- 其次,针对重要的会计科目,明确所有相关的财务报表认定[1],并选择相关需要进行评估的业务流程。因为选定的会计科目很多,所以一般来说,前述章节中说明的各领域基本上都会被作为评价对象。
- 在有着良好的公司层面内部控制的前提下,使用关键财务指标(Key Financial Measure,例如,用销售额、净利润和总资产三个指标),选择需要纳入 SOX 法案内控准备范围的分支机构或业务地点。一般来说,选入的分支机构或业务地点应当要占到该三个指标的"主要部分"。一般在实务中占每个关键财务指标的 60%—70%。

但是,根据 2007 年 6 月公众公司会计监督委员会(PCAOB)颁布的

审计准则第5号(AS5),该文件强调了风险导向方法的重要性,企业自我评估以及外部审计的评估对象可以更侧重于承担风险的项目。

日本版SOX大致的评估范围选定程序如下:

- 首先,评价公司层面控制(以公司层面控制为基准)和财务决算流程。
- 其次,选择需要对业务流程实施评估工作的重要分支机构。《实施标准》中举例道:"当公司层面控制良好时,选择销售收入的2/3",大部分的企业都据此选择。美国SOX法案的实务中,一般标准是销售收入、资产、利润这三项;与此不同,日本版SOX仅为销售收入,理论上可能有些牵强,但值得注意的是,以这样的标准选定的分支机构的数量相比美国SOX法案来说会大大减少。
- 在重要的分支机构,要把'基于公司经营目标非常相关的重大科目所涉及的业务流程'选为评价对象。《实施标准》中,与公司经营目标关系密切的会计科目举例来说包括如下内容:"对于一般企业来说,是销售收入、应收账款和存货",与存货这一科目相关的业务流程是'销售流程、仓库管理流程、期末存货结算流程、采购流程、与存货相关的成本计算流程"。尽管如此,广大的公司应该把这些内容作为示例来看待。
- 在上述内容之上,应当在对财务报表有着较大风险的业务流程,需要追加个别的评价对象,而这与2/3的选定原则没关系:

  a."与风险较大的交易相关的业务流程"

  ……例如,金融交易和衍生工具交易。

  b."与管理层估算或者预测相关的重要科目所对应的业务流程"

  ……例如,预提费用和固定资产减值准备,递延税款的借方或者贷方余额。

  c."非常规性的、不规则的交易发生虚假记录的风险较大,因此需要特别关注的流程"。

中国版SOX在很多方面还未在实务上有定论,目前很多企业参照美

国 SOX 法案实施。

▼ 格式样表和指导手册的制定

确定评价范围之后，下一步就是确定评价用的格式样表。特别是作为文档核心成果之一的风险控制矩阵应该包含哪些信息，这是大有讲究的。风险控制矩阵的格式样表中，应该体现财务报告的风险一览、对应的需要实施的标准内部控制活动举例等，然后应随着文档化工作的开展，在各个分支机构把现场的实际控制活动记录下来[2]。

为了完整性起见，如果风险控制矩阵包括更多的内部控制条目，则可能会识别出更多的内控问题点。但是另一方面，条目多的风险控制矩阵可以在某条内部控制没有得到有效设计和运行的情况下，较容易发现有其他补偿性控制活动可以满足同一个风险或者控制目标，这样的话也是没问题的。这种做法的不利之处在于，文档化和测试的工作量自然就大了，特别是每年都需要开展的文档更新和测试工作。所以，仅是为了“要自己安心”就尽量设比较多的内部控制条目也是要不得的，关键是在专业判断之下，追求工作效率和效果间的平衡。

在设定比较少的内部控制条目的情况下，文档化和测试的工作量固然可以减少，也有助于整个集团管理的一致性和可复制性。但是，由于这一较少的控制活动刚好满足风险和控制目标的要求，则对于记录下来的内部控制活动（或者其补偿性控制活动）的不折不扣地运行就尤为重要。此外，条目减少之后，对于财务报表的认定和相应的财务报告风险的覆盖率是必须关注的一个问题。

在设置内控条目的时候（有时候是根据审计师等提供的通用内容进行调整），要注意项目成员往往会有把自己过去在某项业务中的经验记录下来的倾向。如本书前面各章节所讨论的，海外子公司实施的内部控制不一定国内子公司会照搬，或者由于业态的不同内部控制的做法是不一样的。公司内部有着各种各样的业务，所以要注意不要因为对特定对象先入为主的推测而影响内部控制记录的准确性。

另外,随着对象业务流程和地点的不同制作多个格式样表的话,整个维护工作就会很麻烦,所以应当尽量避免。公司应该尽可能地在全体子公司使用一个统一的格式样表,实在遇到个别地点有非常特别的业务的时候,再为其个别制作特别的内控文档,这样的安排是最为恰当的。

此外,公司应当使项目根据业务流程的流向开展,尽可能地使用记录方便、阅读明了的格式样表来指导内部控制的文档化工作[3]。

笔者所属的会计师事务所一般推荐使用风险控制矩阵这个模板,在其他一些会计师事务所,也存在不使用模板,而是采取对各分支机构所存在的风险进行完整彻底的讨论,并在此基础上找出实际存在控制的方法。由于不同的国家或地区可能存在特定风险,所以这样的方法有一定的优点。但是,缺点是记录内控文件的工作比较麻烦,且容易造成只罗列已有的业务,没有充分识别潜在的风险。还很有可能导致内控文件记录的结果就是大致没有风险。

在有部分或者全部的内控文档化和测试由现场业务部门实行的场合,项目组一方面应该有"指导手册"帮助其履行该项工作,指导手册的内容和规则应当浅显易懂;另一方面,应当对现场的工作组成员给予更加详细的指示或者补充说明,两者相结合起来效果会更好。

▼ 软件的使用

现在市场上有着越来越多的支持美国 SOX 法案和日本版 SOX 应对的软件,现在也由于中国版 SOX 的推出,逐步进入中国。大致来说,公司在内部控制相关的工具软件使用上有以下三种形态:

(1) 不使用任何内部控制相关的软件;

(2) 使用内部控制相关软件来管理做好的内控文档和测试底稿,类似于档案管理软件;

(3) 使用内部控制相关软件来制作内控文档和运行测试,并且开展动态管理和追踪。

最近的趋势表明,由于内部控制与风险管理的紧密联系,有部分的内

控相关软件从以上第三种形态进一步进化成为风险识别、评估、应对管理和风险内控自我评估和预警的风险控制软件，为那些希望追求系统集成管理的大型集团所推崇备至。

在上述的第二种形态下，在实际操作上与第一种形态类似，先用Word或者Excel等电子文件完成文档和测试，然后把这些确认好的内容集中上传，或者逐个贴到某个信息档案管理软件中。简而言之，围绕让管理层（内控的评价者）和外部审计师使用方便的目的，使用软件收纳、管理相关信息，这样在软件上的花费就不会很多。可以想象，如果外部审计师可以在自己办公室直接从国际互联网上下载该公司的主要内控文档和测试结果的话，将是何等的便利。

在上述第一种形态下，即使不使用任何内部控制软件也能把内部控制相关法案准备工作完成得很好的公司大有人在。作为外部审计师，经过整理的清晰的内容是最重要的，而不是说，没有内控软件就难以开展内控评价。另外，不管有无使用内部控制相关软件，测试证据还是较多使用纸张来保存的。

在上述第三种形态下，项目组和现场业务部门的担当人员可以直接在内控软件的界面上操作，尽管相对需要花费较大的成本，但如果可以熟练使用的话，项目效率会有很大提高。在考虑费用效率比之后决定导入内控软件的公司，与其在项目推进方式决定之后再上内控相关的软件，可能会比较花时间，倒不如把项目推进方式与内部控制软件的构想结合起来考虑会比较好。

注

[1] 所谓“认定”，是“为了制作恰当的财务信息所必须要达成的要件”。换而言之，当重要的会计科目的认定没有达成的时候，就是财务报告风险。例如，销售的真实性不具备、应付账款不完整、应收账款估价不准确等。美国SOX法案的《审计准则》、日本版SOX《实施标准》，

以及各审计师自己的审计手册中对此均作了一些规定,尽管略有差异,但是大同小异。美国 SOX 法案《审计准则》定义了存在与发生(Existence or Occurrence)、完整性(Completeness)、估计和分摊(Valuation or Allocation)、权利和义务(Rights and Obligations)、表达和披露(Presentation and Disclosure)五个认定。日本版 SOX《实施标准》定义了真实性、完整性、权利义务的归属、估价的准确性、会计期间截止性、披露和表达的恰当性六个认定。笔者所属的会计师事务所定义了真实性(Validity)、完整性(Completeness)、正确性(Recording)、会计期间截止性(Cutoff)、估价的准确性(Valuation)、披露和表达的恰当性(Presentation)六个潜在的风险(相对于五个认定)。

在中国的《企业内部控制鉴证指引》(征求意见稿)第十一条中有如下表述:"注册会计师应当根据风险评估结果,确定重要的账户、列报和相关认定,选择拟进行测试的控制,以及确定针对特定控制所需收集的证据。"然而,指引没有对具体应该考虑哪些认定作出定义。一般认为中国在实务中会按照普遍认可的定义来实施。

[2] 内控文档过程中记录较多内部控制条目的情形下,需要进一步选定"关键控制活动"(即可以减轻财务报告风险的重要控制活动,在日本版 SOX 中称为"控制要点")。其次在关键控制活动中,还可以区分首要的(该关键控制活动可以直接把某项财务报告风险减低)和次要的(需要与其他关键控制活动结合起来才可以把某项财务报告风险减低)两类。当在内控文档中记录较少内控条目的情形时,关键控制活动的判断已经完成并体现在文档中,同时应当要求严格遵照执行。

[3] 内控文档化的工作应把实际实施的内部控制内容记录下来,形成流程描述。而那种把内部控制实施的情况下就算"○";没有实施的时候算"×"的"○×式"的内控文档一般来说是过不了关的。"○×式"内控文档由于不包括实际是谁、隔多久、使用何种表单等信息,很容易被认为是内控文档不健全。

专栏　中、美、日内部控制相关规定的概要

• 美国 SOX 法案相关规定的概要

Sarbanes-Oxley Act（萨班斯—奥克斯利法案，简称“美国 SOX 法案”）：是一部关于企业财务报告披露的法案，于 2002 年通过。其中的 404 条款中规定，上市、发行公募债券的企业经营者须对内部控制进行评价并报告，外部审计师须对对象企业的内部控制进行审计。

审计准则：PCAOB（the Public Company Accounting Oversight Board：SEC 下设的监督 SOX 法案执行情况的机构）制定的审计准则第 1 号至第 6 号。其中 2004 年 3 月公布的审计准则第 2 号（AS2：An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements）用了 200 页左右的篇幅确定了外部审计师应实施的内部控制审计的具体内容。对美国 SOX 法案而言，起初没有与经营者评价有关的标准，而 AS2 发布以后便成为了事实上的标准。

美国审计准则公告第 5 号（AS5：An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements and Related Other Proposals）的草案于 2006 年 12 月出台，2007 年 5 月正式发布。第 5 号准则对第 2 号准则的内容进行了大幅的修订。最重要的变化是，高度强调采用自上而下原则和风险导向原则，允许外部审计师（和经营者）采用更灵活的应对措施。另外，取消了原来的间接报告和直接报告两种形式并存的审计意见，统一为只采用直接报告的形式。

SEC Rule Guidance：SEC 也发布了各种与 SOX 相关的规定和指导。其中比较重要的是，在美国 SOX 法案基础上于 2003 年 6 月公布的规则、2006 年 12 月出台的草案以及 2007 年 5 月正式发布的经营者评价准则（为了与 AS5 同步）。此外，SEC Rule 规定了不同种类企业适用美国 SOX 法案的时间。

• 美国 SOX 法案的适用对象和适用时间

提前适用的企业(Accelerated Filer:在美国上市、发行公募债券的大中型企业,约 4 000 家)。在 2004 年 11 月 15 日之后结束的财务年度开始执行。在美国,每年 12 月进行财务决算的企业比较多,因此 2004 年 12 月末便成为了首次出具内部控制报告的基准日。

外国企业(Foreign Private Issuer)。适用日期被再三推延,最终确定 2006 年 12 月 15 日以后结束的财务年度开始执行经营者评价,2007 年 12 月 15 日以后结束的财务年度开始适用外部审计。

小规模企业(市价总额不满 7 500 万美元的上市公司,约 7 400 家)。这些公司的适用日期也被再三推延,最终确定 2007 年 12 月 15 日以后结束的财务年度开始执行经营者评价,2008 年 12 月 15 日以后结束的财务年度开始适用外部审计。

• 日本版 SOX 相关规定的概要

金融商品交易法:2006 年 6 月订立,对以前的证券交易法进行了大幅度更正的重要法案。其中,对经营者内部控制评价报告和外部审计进行了规定,并且明确了对象企业和适用时期。

内阁府令:2007 年 8 月公布,当年 8 月下旬公布了指导草案。共 24 页,规定了经营者内部控制报告书的格式。

标准(财务报告相关的内部控制评价以及审计标准):日本金融厅企业会计审议会于 2005 年 12 月公布了暂定版。2007 年 2 月发布了最终确定版,共有 21 页,阐述了日本导入内部控制评价制度的初衷,以及相关的概要内容。

实施标准(财务报告相关的内部控制评价以及审计相关的实施标准):日本金融厅企业会计审议会于 2006 年 11 月公布草案,2007 年 2 月与"标准"一同发布。实施标准用了 90 页左右的篇幅,具体说明了经营者的内部控制评价以及外部审计的相关要求。

实务方针(财务报告相关的内部控制审计的实务处理):2007 年 7 月,由日本注册会计师协会公布草案,同年 10 月定稿。与内部控制相关的审计标准内容有 80 页左右。其中有 20 页左右的内容,是与内部控制的审计结果相关的,合并财务报表的审计报告样本。

Q&A:日本金融厅在 2007 年 10 月发布了 20 个问题集,之后于 2008 年 6 月追加了 46 个问题,合计共 67 回问答。2008 年 3 月,发表了 11 个错误的理解。主要是为了说明日本版 SOX 不是为企业增加不合理的负担,以及列举更具体的判断数值等。

• 日本版 SOX 的适用对象和适用时间

所有的上市公司(约 3 800 家)都属于适用对象企业。从 2008 年 4 月 1 日以后开始的财务年度起执行。由于日本企业主要在 3 月份进行决算,因此将 2009 年 3 月 31 日定为最初的内部控制报告基准日。

• 中国新公布的内部控制相关规定

2008 年 6 月 28 日,内部控制相关的新规定出台。财政部等五部委联名下发了《五部委关于内部控制的通知》(财会[2008]7 号,以下简称《通知》),以及作为附加资料的《企业内部控制基本规范》(以下简称《规范》)。与此同时,财政部办公厅也发布了《企业内部控制应用指引》(以下简称《应用指引》)、《企业内部控制评价指引》(以下简称《评价指引》)、《企业内部控制鉴证指引》(以下简称《鉴证指引》)这三个指导文件的征求意见稿。

• 《通知》的主要内容

通知仅 2 页,主要确定了如下方针:"上市企业从 2009 年 7 月 1 日起,必须对企业自身内部控制的有效性进行自我评价,并披露年度自我评价报告(鼓励非上市的大中型企业执行)。"

对于外部审计,《通知》进行了如下的说明:"可聘请具有证券、期货业务资格的会计师事务所对内部控制的有效性进行审计。"

制度的正式执行是在公布之日起的1年以后,间隔时间较短。不过何时"正式"开始企业的自我评价和外部审计师的审计并没有明确。换言之,由于从制度出台到实施的期间较短,企业现实面临的是,"应该应对到何种程度?""以及在什么时机进行应对?"等问题,这些还需在今后加以明确。

·《规范》的主要内容

《规范》一共13页,由七大章五十条构成。第一章总则的十条内容阐述了内部控制的基本概念和重要原则等信息。

总则中的第二条写道:"本规范适用于中华人民共和国境内设立的大中型企业。"这意味着,《规范》中所指的"理想的内部控制"的适用对象是大中型企业。从费用和效果的角度来看,小规模企业如果执行理想的内部控制的话,有时可能会违反成本效益原则。美国SOX法案的AS5中也到处写着需要对小规模企业给予照顾。

另外第十条规定说:"为企业内部控制提供咨询的会计师事务所,不得同时为同一企业提供内部控制审计服务。"值得关注的是,在美国和日本的实务中,外部审计师在不违反独立性的范围内,可以提供咨询服务。而在"规范"中提到的关键字"同时",我们或者可以把它理解为"只要不是同时进行就可以"。这点尚待监管机构进一步予以明确。

第二章至第六章从内部控制的各个基本要素出发,列举了应该具备的公司层面控制的内部控制(第二章:内部环境9项、第三章:风险评估8项、第四章:控制活动10项、第五章:信息与沟通6项、第六章:内部监督4项),合计一共37项内容。

·《应用指引》的主要内容

《应用指引》全文共163页,针对22个业务领域,列举了相关领域中所要求的内部控制。《规范》中主要规定了公司层面内部控制,而《应用指引》主要是针对业务流程层面。

- 资金
- 采购
- 存货
- 销售
- 工程项目
- 固定资产
- 无形资产
- 长期股权投资
- 筹资
- 预算
- 成本费用
- 担保
- 合同协议
- 业务外包
- 对子公司的控制
- 财务报告编制与披露
- 人力资源政策
- 信息系统一般控制
- 衍生工具
- 企业并购
- 关联交易
- 内部审计

因为《应用指引》涵盖很多内容，在实务操作中，与其说是要求企业全盘按照《应用指引》上述所有内容来设计执行本企业的内部控制，倒不如说《应用指引》列举的这些内部控制可以作为各企业参照的范例。今后，中国的企业需要更加重视《应用指引》的相关内容。

•《评价指引》的主要内容

《评价指引》全文共 10 页，规定了管理层执行内部控制评价的基本原则。从内容上来看，其实务操作与美国 SOX 法案和日本版 SOX 没有很大差异，可以说是汲取了内部控制评价的精华。换言之，针对中国上市公司的管理层，也要求其执行类似于美国 SOX 法案和日本版 SOX 的内部控制评价方法。

以下是我们应关注的地方：

“根据风险发生的可能性和对企业单个或整体控制目标造成的影响程度来确定需要评价的重点业务单元、重要业务领域或流程环节。”（第五条）

⁘ 在美国 SOX 法案中，AS5（美国审计准则公告第 5 号）中也明确了风险导向原则。

"企业实施内部控制评价,包括对内部控制设计有效性和运行有效性的评价。"(第十条)

"应用信息系统加强内部控制的企业,应当对信息系统的有效性进行评价,包括信息系统一般控制评价和信息系统应用控制评价。"(第十一条)

"内部控制评估和测试的方法主要包括:个别访谈法,调查问卷法,比较分析法,标杆法,穿行测试法,抽样法,实地查验法,重新执行法,专题讨论会法。"(第十八条)

⁘ 关于评价方法,我们可以感觉到监管当局的要求(并非局限于抽样法)更加多样化,允许采用更灵活的评价方法。

"内部控制缺陷分为一般缺陷、重要缺陷和重大缺陷。"(第二十六条)

⁘ 该定义沿袭了美国 SOX 法案的内容。

"内部控制评价报告至少应当包括下列内容:(中略)(六)被评估的内部控制整体目标如果无效,存在的重大缺陷及其可能的影响。"(第三十一条)

• 《鉴证指引》的主要内容

企业内部控制鉴证指引全文共 23 页,前 15 页中描述了关于注册会计师对于内部控制鉴证业务的原则。后 8 页是关于内部控制鉴证报告的格式。参考中有如下四种报告:标准鉴证报告(无保留意见),带说明段的无保留意见鉴证报告,否定意见鉴证报告,无法表示意见鉴证报告。

此外,鉴证报告中对于公司的内部控制直接发表意见(美国 SOX 法案中,根据 AS5 的要求,也是采取直接发表意见。日本版 SOX 中所规定的是采取间接发表意见的形式,注册会计师对于"管理层评估结论是否妥当"进行发表意见)。

以下是我们应关注的地方:

"对企业与财务报告相关的内部控制的有效性进行鉴证,并发表鉴证意见。"(第二条)

“即使财务报表不存在重大错报，内部控制也可能存在重大缺陷。”（第六条）

“企业组织结构、经营单位或流程的复杂程度可能影响企业实现控制目标的方式。（中略）注册会计师应当根据企业情况调整工作范围，以获取充分、适当的证据，支持发表的意见。”（第十四条）

⁘ 该条包含了考虑到规模较小的上市公司，在鉴证取证上留有一定余地的内容。

“如果企业有多个经营场所或经营单位，注册会计师应当在评估与经营场所或经营单位相关的财务报表发生重大错报风险的基础上，确定拟对哪些经营场所或经营单位实施控制测试以及如何进行测试。”（第十五条）

⁘ 在《评价指引》和《鉴证指引》中，都未具体明确如何选择测试子公司或单位。

“注册会计师应当测试企业是否存在对内部控制具有重要影响且有效的企业层面控制。注册会计师对企业层面控制的评价能够增加或减少其本应对其他控制进行的测试。”（第二十条）

“注册会计师应当识别重大的账户、列报及相关认定。”（第二十六条）

⁘ 要求注册会计师识别重大账户等，这一点值得探讨。（在相关指引中并未特别述及公司管理层是否自己也需要识别重大账户、列报以及相关认定，而是指明由注册会计师去执行。）

“注册会计师应当测试对得出控制是否有效结论有重要影响的控制。”（第三十五条）

“控制测试需要涵盖足够长的期间。”（第四十五条）

第十九章 内部控制项目的展开（2）推进和定性

项目管理（课题、任务、工时及进度管理）必不可少

推进阶段 根据各分支机构的实际情况灵活改变推进的方法

应对内部控制报告制度的要求，就是开展一项与公司规模相当的项目，所以“项目管理”是必要的。这包括课题管理、任务管理、工时和进度管理等。我们必须对于工时不足和拖延进度的项目预先制订计划；对于可以省去的项目、可以延后做的项目、反之不得不遵守的项目等进行优先顺序排序，然后做出相应的安排。

▼ 分不同分支机构来应对

在推进过程中，对于各分支机构的不同情况，适当改变推进方法的灵活性是很必要的。所谓“不同情况”，比如说，“分支机构是否能有所帮助”、“母公司的影响力是否强大”等，特别对于海外分支机构来说，就是“是否采用本地的外部资源”、如果采用的话“外部资源和母公司的外部资源是否相同”，并且“当地的管理者和员工和派驻海外员工中谁来做多少事情”、“是否为所有人”、“是否进行实际操作”等情况。

对于海外分支机构，语言也是一个问题。美国 SOX 法案和日本版

SOX 中有“经营者评价”的制度，而在中国的内部控制报告制度（中国版SOX）中也要求管理层的内部控制自我评价。所以，理论上内控文件和内控自我评价的语言应该是经营者、管理层能够读懂的语言，在实际上也最好是代表管理层进行内控项目的成员能够读懂的语言。然而，实务中，在准备满足内部控制报告制度的海外分支机构中，对母公司报告用的问题点清单就需要用管理层能够读懂的语言来制作，这是最低要求；而其他的成果可以用当地语言写。

从经验上来说，美国 SOX 法案下，总部要求海外子公司用英文进行内控评价的记录，但遗憾的是，用英语编写成果最困难的往往是日本的子公司。在日本版 SOX 下，日本企业的欧美子公司和东南亚的子公司可以用英文来记录，但中国子公司一般无法使用英文，大多数是使用中、日双语来记录内控评价。中国版 SOX 下，由于目前暂时在海外拓展业务的上市公司不多，所以还是以中文为主。

如果在海外分支机构采用当地的资源的情况下，一方面可以缓和语言和路途遥远的问题，但是另一方面总部管理其支持内容的工作也很辛苦。欧美企业非常重视沟通，定期举行电话会议、视频会议（虽然我们最好也能够这么实施，但是用英语的会议还是很累的），并且对于做法模糊的地方进行细问也很辛苦。

不管怎么说，因为是海外，推进方法有差异也是没有办法的事。需要遵守的最低限度的原则就是“清晰传达要求”，并也需要容许与之相异的风格。

一般来说，内控项目最好能用集团全体统一的推进方法来进行评价；但是在集团内有大的子公司，或者其分别上市的情况下，往往需要用与母公司不同的方式方法来推进内控项目。

海外子公司使用外部资源的服务费用应该是由母公司还是由子公司来承担，一直是一个讨论的话题。在美国 SOX 法案的准备工作中，母公司大多会考虑全球的预算；而在日本 SOX 中较多的情况是，各子公司分别进行应对。还有母公司仅承担特定子公司的费用的情况，但这会产生

不公平感，所以很难处理，故就子公司的个别情况进行适当的判断就显得很重要。在应对中国版 SOX 的准备工作中，由谁承担费用的问题并不突出，原因可能是中国上市公司的国际化步伐并不明显所致吧。

▼ 内控文件编写的心得和文件成果

企业进行内控文件编写之前，首先需要在评价对象的分支机构中进行会计科目的分析以及对应业务流程、子流程的识别。这时，对于业务流程应该适用什么模板就成了问题。原则上，应将实施内部控制中差异很大的业务(例如对公司销售和对个人销售并存)分别编写内控文件，将相似的业务(例如仅是制品类别的差异)归总后进行内控文件的编写。但在实务中往往会有不同的考虑。如，有时会由于不同的部门有不同的负责人，而将各自内控文件编写的工作进行分离比较合适。又如，通常各公司不同的情况下，内控文件的编写是各自进行的，但对于把一部分业务流程委托给集团内部，以及对于仅为方便或某种目的而设立的其他无实际业务的企业(如皮包公司等)的情况下，适合的做法反而是将若干家公司的业务归集后再编写一套内控文件。这些注意点在内控文件编写开始之前不对其进行适当确认的话，就可能无法分清工作对象而造成混乱。

内控文件的成果一般就是“风险控制矩阵”、“流程图”以及“业务流程描述书”这三点。此外，也会制作“问题点清单”和其他的报告资料。

美国 SOX 法案应对中经常可见到的说法是，风险控制矩阵和业务流程描述书在实质上内容相同(而且都写得非常细)。(笔者个人)推荐业务流程描述书中记载那些作为理解内部控制的背景的业务概要，例如组织结构和主要的业务系统，销售循环中主要的销售渠道、客户、商品构成、应收账款回收方法和回收条件等内容。这样有助第三方的理解而能够避免内容的重复。

风险控制矩阵是内控文件中的最重要的成果，一般记述了对于潜在的风险，哪些是应该实施的内部控制；但更详尽的内容在业务流程描述书中记录，风险控制矩阵可以认为是从其抽出一部分最核心内容而构成的。

流程图依据编制人员的能力、品质要求和所需时间相差甚远。一般公司多倾向于就销售和采购制作流程图，往往不制作（不适用）财务决算和 IT 全面控制的流程图。

▼ 文件编写的实施者

可以考虑用下面的模式来决定由谁实施文件化。

（1）项目成员实施。

（2）现场部门实施，项目成员对其支持[1]。

项目成员实施的情况下，项目成员工时花费是难免的，但相应的好处是，由于是由理解项目目的和推进方法的成员进行，项目的进度很快。（应对美国 SOX 法案的第一年，即 2004 年的下半年，工作迫在眉睫，许多公司将十万火急的内控文件编写和内控评价委托外部资源进行，非常辛苦。）

就算是项目成员实施的情况下，在内控文件编写时现场部门至少也会发生应对访谈的工时。特别在欧美企业及其子公司，管理部门对于效率抓得很紧，在这种追加的工作上花时间，可能不会很积极地予以配合。

另一种方法是，由现场部门进行内控文件编写，现场部门对项目的目的和推进方法进行了解、实施编写后，将其结果交由项目成员复核后进行访谈。这样做项目进度肯定比较慢，并且为了控制质量也需要花费时间。但是，因为内控自我评价是连续性的活动，公司在适用的首年度开始建立内部控制的意识，可以预想之后年度的工作就可以更顺利地开展。在项目成员实施的情况下，尽管深入理解流程并且适当地进行了访谈，记录那些应记述的例外事项等还是很难的。通过这项工作固然要制作成让外部审计看得懂的内控文件，但是内控实施者自己却不理解的话就很奇怪，所以还是希望现场部门适度地参与内控文件的编写工作。

就算让现场部门进行内控文件的编写，项目成员也要拥有审计的视点，是否有没有记述的例外事项？是否有本人没有意识到的问题点？这些事情必须要确认。此项工作不仅只是围绕着内控模板在表面上编写内

控文件，而是在理解对方业务和辛苦的同时，尽量提及关联业务中可以进一步提高效率的内容，帮公司“打通血脉”，这才是有价值的事。此外，由于项目中会向各部门、子公司进行访谈和询问，这是很好的经验。

文件化实施后，最好进行穿行测试(设计状况的评价)。穿行测试是指，为了确认文件中设计好的内部控制是否确实实施并加以运行，获得实际采用的凭证和表单，对于交易的流程进行确认。一般来说，可以在项目成员进行内控文件编写时，将穿行测试和文件编写并行；或者在现场部门自行进行编写内控文件的场合，为了确认其内容，向现场部门进行访谈时进行穿行测试比较合适[2]。

▼ 内控运行情况的评价(验证)

所谓内控运行情况的评价，也就是内控运行验证或测试，是检查内控文件记录下来的“应实施”的内部控制，是否如其所述在运行。通常可以通过内部单据抽样等来证明，这里就不详细展开了。判断证据收集是否足够的原则是，有必要收集让第三者看了也能够得出同样结论的证据。

在内控运行验证中，尽管常有发现漏盖章、证据文件保管遗失等纯粹的内控运行的缺陷，但更多的是会发现没有像内控文件记录的那样去运行的内控缺陷(特别是在没有充分实施穿行测试的情况下)。这意味着，内控设计缺陷和内控运行缺陷的界限很模糊。如果 10 个样本中有 1 个例外(违反规则)的话，那是内控运行的缺陷；而如果 10 个样本中 10 个样本都没有运行，就是根本没有控制，是内控设计的缺陷[3]。

在日本版 SOX《实施标准》中，“企业层面的内部控制评价结果是有效的话，对业务层面的内部控制评价时，可以采用缩小样本量等更为简单的评价手续，在判断重要性水平的基础上，对于评价范围的一部分，把多个会计期间合并作为评价对象”。正如第十四章和第十八章所述，一定要努力让实务中“企业层面的内部控制有效”，达成这个目标的公司在日本版 SOX 中会被容许取更小的样本(前提是更低的信赖度)、允许使用轮换测试计划。

在中国版 SOX 中的《企业内部控制鉴证指引》(征求意见稿)中,也表达了类似的意思,强调企业层面内部控制的重要性,以及可以采用轮换测试计划。“第二十一条(二):某些企业层面的控制能够监督其他控制的有效性。当这些控制运行有效时,注册会计师可以减少对其他控制的测试”;“第五十条:注册会计师应当每年改变控制测试的性质、时间和范围,以增加测试的不可预见性并能够应对环境的变化”。

美国 SOX 法案的审计准则第 5 号(AS5)所要求的“自上而下”的工作流程,以及“风险导向原则”,使得评价对象范围的选定更加灵活,需依赖专业判断;但是轮换测试计划经过讨论还是不被允许。

顺便说一句,轮换测试中有分支机构的轮换测试、(同一分支机构中的)业务流程的轮换测试、(同一业务流程中)内部控制活动的轮换测试。即使允许使用轮换测试计划,对于重要的分支机构、业务流程和内部控制活动,还是需要每年纳入考虑的。同时,活用轮换测试计划让此项工作负担变得轻松也是很关键的。

关于内控运行测试的实施者,也可以分为项目成员实施,现场部门实施、项目成员提供支持两种。由于验证对独立性有要求,如果可以的话应在部门间进行,至少要考虑到不能让实施内部控制行为的当事人进行验证。

实施者的独立性是外部审计师能够多大程度上信赖公司的评价的要素之一,所以和内控文件编写相比,最好能够让项目成员或者内部审计部门进行内控运行测试。

并且,作为文件化和评价展开的方法,有如下两种:

(1) 在多个分支机构中展开内控文件编写,然后分别评价的方法;

(2) 限定先行的试点分支机构,进行内控文件编写,然后在该分支机构继续进行运行评价(以及问题点的判断)的方法。

在方法(2)的场合,如果时间充裕,最好可以让项目成员在一个分支机构将整个内控文件编写和评价的流程了解清楚后,再推广到其他分支机构进行。但是在实务中,因为项目日程比较紧,在一个分支机构内控文

件编写完毕后，项目成员往往需要开展其他分支机构的文件编写，同时准备运行测试，这种情况很多。

▼ 内控缺陷的判断和整改

通过内控文件记录和内控评价可以发现各种内部控制上的缺陷(不完善或问题点)，下一步就是要对于这些问题一一理解、判断是否需要整改。

正如前文所述，不是重大缺陷就不整改的做法是不能令人满意的[4]；但是反过来说，就算是很小的缺陷也进行整改的做法也有些过度。考虑到问题大小和整改所需费用、工时的平衡，即使缺陷不是很大，但若是公司管理必须做的事项，且费用也不大，就可以进行整改。所谓整改，往往可能需要部分改变实际正在执行的业务流程，所以有着与内控文件编写和内控评价不同的辛苦之处。此外，如果是一个要从正面整改、需要花费很大的费用和很长的工时的内控缺陷，不妨考虑采取用较少的工作负担来减少该问题的风险的折中手段。

但是，上述对于内控缺陷如何进行判断，实际上还是很主观的。例如，如果存在“对于销售价格的折扣批准不彻底”的问题，就很难估计对于销售收入、应收账款有多大的影响[5]。因此，很难对在何种场合下作出何种判断进行明文规定。而且，对于相同的一个内控缺陷，对A事业部要求整改，但是对B事业部不要求，这样做会使情况变得更乱。

在实务中，大企业的内控报告制度应对项目的过程中所碰到的问题也有限，所以较为实际的做法是让特定的责任人(小组)对所有的问题进行统一判断。这个责任人需要有平衡感，对于内部控制的重要性有良好的认识并且对企业的业务有很好的理解。并且，这位负责人要不迎合各分支机构，能够从内部审计视点出发，对于应该做到的事对各单位作出明确的要求。

但是，内控缺陷的判断和整改通常不是在内控文件记录和内控评价全部完成后进行的。因为对设计有问题的内部控制，进行运行测试是没有意义的。在内控文件记录和穿行测试的阶段中对于明确知道有问题的

内部控制应当着手进行改善，并且让整改后的内部控制运行一段时间后，再进行内控运行的第二轮测试评价。就笔者所经历过的美国、日本和中国内控报告制度对应项目来看，在时间紧迫的项目中，这种平行开展的情况是很常见的。

笔者的建议是，在实务中不要匆忙判断某个发现的内控缺陷是否属于“重大缺陷”，而是应该预见性地判断问题点的大小来开展整改，然后仅就整改中的难点和最终测试仍然不合格的地方等，从公司或集团整体角度，再来判断是否属于重大缺陷。

实务中，这个预先判断多可分为大中小（或者 High，Medium，Low）三档，也可由公司分为大小两档。但对于分为两档的情况，很可能造成决定整改大的地方、放弃小的地方的情形。

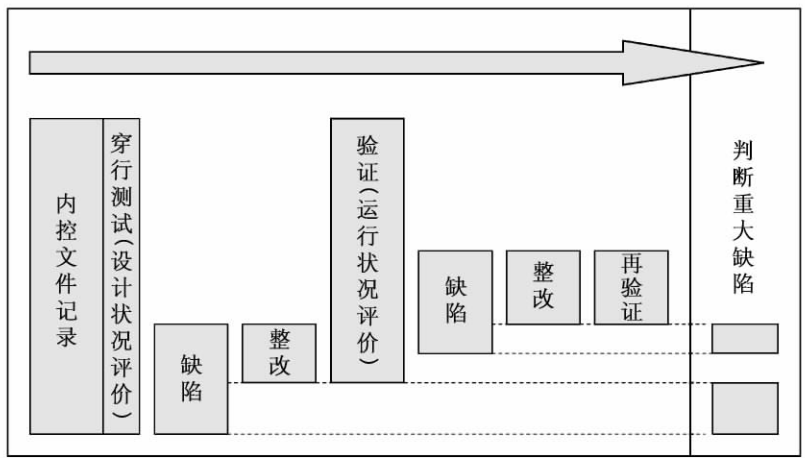

图 19-1　内控文件记录、整改、验证的一般流程

定性阶段：与外部审计师坦率磋商

▼ 外部审计师的内部控制审计

接下来，正式的期末大考开始了！

因为外部审计师的任务就是发现问题，就算公司再怎么准备，也会被指出有不完备的地方。

外部审计师也会指出对于公司准备中未发现的问题。外部审计师可能会对公司已经发现问题的性质作出更严重的判断，因为问题点大小的判断，如前所述主要是主观的。此外，由于外部审计师的时间也很紧张，在确认大量的文件化验证结果的时候也可能产生误解。

作为公司，不用慌张，重要的是首先向审计师说明是基于什么考虑和方法来实施内控文件编写和测试评价的。对于缺陷(和之前内部控制项目上进行的事项相同)，我们要充分分析对财务报告的影响、采用什么整改措施较为妥当，和外部审计师进行坦率磋商。

并且，在各国内部控制相关法规和标准中，内控是一个时点的概念。中国版 SOX 下，《企业内部控制鉴证指引》(征求意见稿)第四十五条中有如下表述："注册会计师在确定测试控制的日期时，应当考虑下列因素：(一)尽量在接近管理层评估日执行控制测试；(二)控制测试需要涵盖足够长的期间。"对于上述的(二)，在接近期末才完成整改的情况下，如果无法提供可以证明内控运行有效的足够证据的话，公司会被认为存在内控缺陷。这是承袭了美国 SOX 法案。

在日本版 SOX 下，"尽管发现重要缺陷，在报告书评价时点(期末)前整改的话，仍然可以承认和财务报告相关的内部控制是有效的"。

▼ 第二年以后的活动

应对美国 SOX 法案，很多公司认为在第一年度只是将内控合规准备都进行一遍就很不容易了，内控文件编写和测试验证也往往不理想，范围不足，品质也很一般。这些企业在内控缺陷的整改上，就算想办法进行改进，也没有很好地贯彻改善，对于小的缺陷的应对则放到了后面。

在第二年，要对第一年各种不理想的事项进行整理。对于连续的管理活动来说，要让 PDCA 循环(计划、施行、检查、执行)形成顺畅的闭循环，在设定总部各部门以及现有组织的组织分工和相应职能的同时，还需

要设定现场部门担当者的组织分工和相应职能。

内部控制报告制度的目的是为了确保财务报告的可信性。除此之外，公司内部也有相似的活动。例如有 ISO9000 和 ISO14000 认证、风险评估、合规活动、企业社会责任（Corporate Social Responsibility，CSR）等。这些其他的全公司的活动与内控合规有着相通的组织和推进方式，所以如果可以彼此整合的话，一方面是可以分散内控合规工作的压力，更重要的是在企业内部不应存在多个不兼容的管理体系，而是应该尽量使用一个体系来满足多种管理目的和需要。这无疑将为企业带来更多的协同价值！

注

[1] 控制自我评估（Control Self Assessment，CSA）狭义地来说是采用研讨会等方式讨论与内部控制相关的问题，在组织内部达成内部控制理念的启蒙和宣传的目的。在本书中，它的定义有所扩大，从字面意思来看，也指现场部门广泛地对自身负责的内部控制活动进行自我评价（文件编写、穿行测试和运行验证）的过程也称作 CSA。

[2] 所谓穿行测试，是外部审计师评价公司内部控制的设计情况的程序，但是公司在自己开展内部控制设计情况评价时也应当实施该程序。特别是对于采用轮换测试计划而轮空不测试内控运行情况的领域，在实务上也很有可能需要开展内控文件的更新和穿行测试。

[3] 进一步区分内控设计的话，美国 SOX 法案的实务中，有两种概念：设计和导入（Design & Implementation）。设计（Design）的概念是“应该存在怎样的内部控制”，导入（Implementation）的概念是“通过规则众所周知”。在中国版 SOX 中，“内控设计”这个词包含了上述两个意思；在日本版 SOX 的《实施标准》中，使用“整备状况”这一术语，意思也是包含了设计和导入的双重意味。

[4] 关于判断控制缺陷大小，在各国的内控法规和/或标准中，均要求按

照金额和性质进行评价。中国的《企业内部控制鉴证指引》(征求意见稿)第二十五条中有如下表述："企业对内部控制评价过程中发现的问题，应当从定量和定性等方面进行衡量，判断是否构成内部控制缺陷。"

[5] 在销售价格的折扣批准不彻底的情况下，公司会认为全部的销售金额的真实性没有保证，或者是有批准但不被认同的销售才没有真实性，还是说仅折扣的部分没有真实性等，判断这些问题的所在是有相当难度的。